Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Kai Yang

Entitled
A Multi-stage Non-cooperative Iris Recognition Approach with Enhanced Template Security

For the degree of Master of Science in Electrical and Computer Engineering

Is approved by the final examining committee:

1. Eliza Yingzi Du
Chair

2. Yaobin Chen

3. Jiangyu Zheng

4. Xukai Zou

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Eliza Yingzi Du

Approved by: Yaobin Chen 06/08/2011
Head of the Graduate Program Date

Graduate School Form 20
(Revised 9/10)

PURDUE UNIVERSITY
GRADUATE SCHOOL

Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:

A Multi-stage Non-cooperative Iris Recognition Approach with Enhanced Template Security

For the degree of Master of Science in Electrical and Computer Engineering

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Executive Memorandum No. C-22*, September 6, 1991, *Policy on Integrity in Research.**

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

Kai Yang

Printed Name and Signature of Candidate

05/20/2011

Date (month/day/year)

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/c_22.html

A MULTI-STAGE NON-COOPERATIVE IRIS RECOGNITION APPROACH WITH ENHANCED TEMPLATE SECURITY

A Thesis

Submitted to the Faculty

of

Purdue University

by

Kai Yang

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science in Electrical and Computer Engineering

August 2011

Purdue University

Indianapolis, Indiana

ACKNOWLEDGMENTS

I would like to gratefully thank my thesis advisor, Dr. Eliza Yingzi Du, for her consistent assistance and guidance during all my courses and research projects related to this thesis work. Without her wholehearted support during the past two years, I would have never discovered the joy of research and finished my thesis work quite smoothly.

I would like to thank my advisory committee members, Dr. Yaobin Chen, Dr. Jiangyu Zheng and Dr. Xukai Zou for their time and help during the completion of this thesis.

I would also like to thank all my lab mates at the Pattern Recognition and Biometric Laboratory, Miss Yan Sui, Mr. Zhi Zhou, Mr. Mike Beale, Mr. Matt Blair and Mr. Yong Lin for their support and help during this chapter of my life. I thank Ms. Valerie Lim Diemer for assisting me in formatting this thesis.

Finally, I thank all my families, who mean more to me than words can possibly express.

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Yang, Kai. M.S.E.C.E., Purdue University, August 2011. A Multi-stage Non-cooperative Iris Recognition Approach with Enhanced Template Security. Major Professor: Eliza Yingzi Du.

Biometrics identifies/verifies a person using his/her physiological or behavioral characteristics. It is becoming an important ally for law enforcement and homeland security. Among all the biometric modalities, iris is tested to be the most accurate one. However, most existing methods are not designed for non-cooperative users and cannot work with off-angle or low quality iris images. In this thesis, we propose a robust multi-stage feature extraction and matching approach for non-cooperative iris recognition. We developed the SURF-like method to extract stable feature points, used Gabor Descriptor method for local feature description, and designed the multi-stage feature extraction and matching scheme to improve the recognition accuracy and speed. The related experimental results show that the proposed method is very promising. In addition, two template security enhanced schemes for the proposed non-cooperative iris recognition are introduced. The related experimental results show that these two schemes can effectively realize cancelability of the enrolled biometric templates while at the same time achieving high accuracy.

1. INTRODUCTION

1.1 Background

Biometrics identifies/verifies a person using his/her physiological or behavioral characteristics [1]. It is becoming an important ally for law enforcement and homeland security. Biometric characteristics can be physiological (such as iris [2], face [3, 4], finger image [5, 6], hand geometry [7, 8], and palm print [9, 10]), behavioral (such as signature [11] and typing rhythm [12]), or a combination of both (such as gait [13, 14] and voice [15]). A biometric system senses a biometric signal, extracts a salient set of features, encodes them into templates, and compares them with the templates existing in a database [16]. A typical biometric identification procedure includes the enrollment stage and the authentication stage. During the enrollment, raw biometric data is fed to the feature extractor; a template is extracted and stored in a database. During the authentication stage, the same feature extraction procedures are implemented on the query biometric signal, and using pattern recognition methods to check whether it is related to its claimed identity in the database (Figure 1.1).

Compared to the traditional authentication approaches (such as password or identification card), biometric is more secure, more convenient to users, and more resistant to fraud. Within all the biometric modalities, iris has been tested to be one of the most accurate biometrics. Iris recognition devices have been widely deployed at airports, government departments, key labs, etc. According to the statistics and prediction of International Biometric Group (IBG), iris recognition will expect a sustainable increment in the near future and the total market of iris recognition technology is going to exceed 700 million USD in 2014. More potential applications related to iris recogni-

tion are expected, especially in public security (criminal detection, surveillance, etc.) and private information protection (access control, e-banking, etc.).

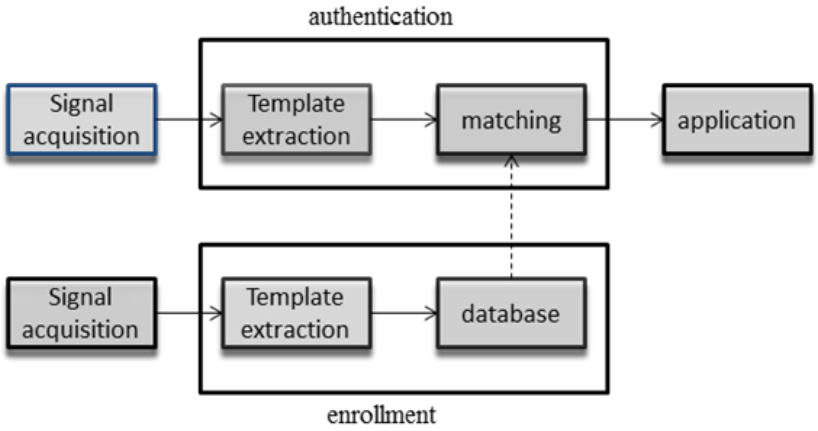


Fig. 1.1.: A typical biometric system

Currently, iris recognition methods can work very well with frontal-looking and high quality images. Within, Daugman's 2D Gabor wavelet approach has been tested and evaluated using large databases, such as the United Arab Emirates (UAE) database with over 600,000 iris images with over 200 billion comparisons [17]. The positive iris recognition requires high cooperation from users, which may make the recognition process inconvenient and ineffective. Moreover, with the more and more increasing requirements of security nowadays, non-cooperative iris is a promising solution for video surveillance and watch list monitoring (identifying wanted criminals or suspects). However, most existing methods are not designed for non-cooperative users and cannot work with off-angle or low quality iris images [18]. First, it is very challenging to accurately segment off-angle iris images. Second, the iris features are often deformed and it is very challenging to perform feature extraction and matching.

Another concern about current commercialized iris recognition systems is the security issue of the traditional biometric systems. The traditional biometric systems are vulnerable to attacks. Ratha *et al.* [19] analyzed all possible attacks to a biometric system (Figure 1.2). Each part of the system, including sensor, extractor, matcher,

database and the channel between them are vulnerable to the danger of Trojan Horse, phishing and overriding templates and results. In the signal acquisition module, attackers can use a fake biometric to fool the user interface. During the transmission, attackers can intercept the signal and replace it with one they recorded before to get invalid access, which is referred to as replay attack. The true features and matching input/output can be tampered during the feature extraction and matching process. The template database and the channel between database and matcher could also be a loophole attacked by hackers. The attackers can even directly change the final result to ruin the system.

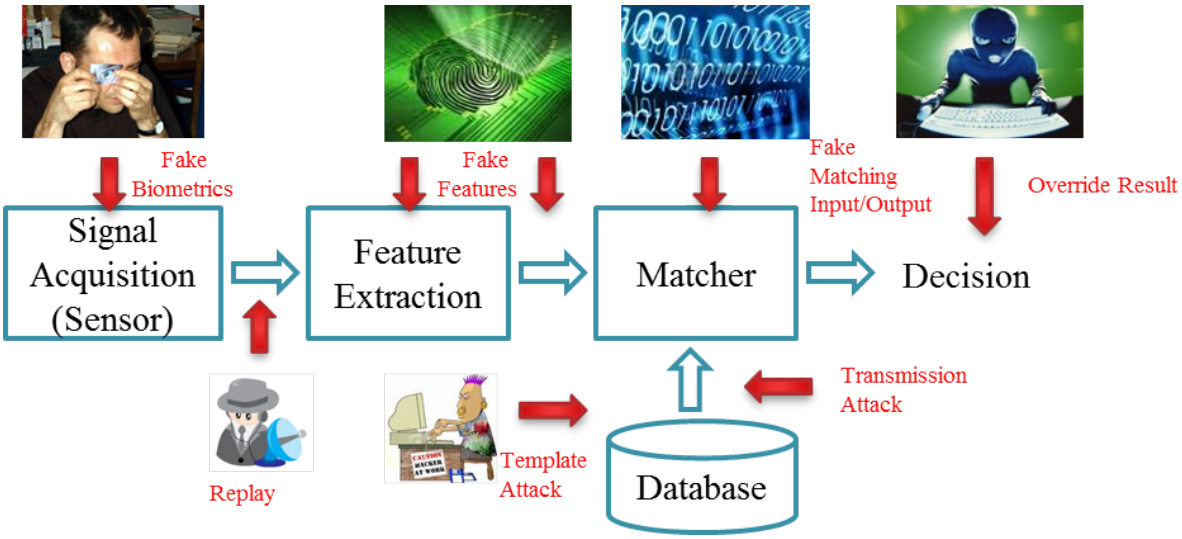


Fig. 1.2.: Possible attacks to a biometric system

Jain *et al.* further summarized these attacks into four types [20]: attacks on user interface, attacks on modules, attacks on channels, and attacks on templates. The most common attack on user interface is the spoofing attack on the signal acquisition module. The adversary tries to fool the biometric system by presenting faked biometric traits to the sensor. Several implementations of liveness test [21–23] in biometric systems have been proposed to deal with this problem. Attacks on modules refer to direct attacks on biometric device modules, including attacks on hardware modules and software modules. For example, the adversary attacks the executable program

using a Trojan Horse [24] to modify the input/output into the value he desires. It is possible to attack the biometric systems on the channels between modules, e.g. intercepting original signals and replaying them with those they intercepted before or fake ones. This will ruin the final matching results or cause the Denial of Service [25] problem. Although the replay attack can be detected by adding a timestamp to the signal [26, 27], it is widely accepted that the encryption and transformation should be implemented from the beginning part of the biometrics identification system, normally combined with the signal acquisition module. Moreover, attacking on the stored templates also leads to serious security and privacy issues therefore arouses the most concern. We will discuss this in Chapter 4.

Unlike traditional authentication methods (password, pin, smartcard, etc.), iris is always binding with user and cannot be replaced once compromised. Algorithms that can ensure the iris template security and replaceability are required for future iris recognition applications. In particular, it is desirable to have a system that can re-generate a new pattern if the one being used is lost, or generate different patterns for different applications to prevent cross-matching.

The objective of this thesis is to study the fundamental issues about iris based authentication methods and develop a fast, robust and effective method to perform non-cooperative iris recognition, while at the same time achieving iris template security and replaceability.

1.2 Organization

The thesis is organized as follow. First, we will focus on the proposed speed-up multi-stage non-cooperative iris recognition method, including Chapters 2 and 3. Related works of non-cooperative iris recognition will be reviewed and summarized in Chapter 2 and the proposed method will be introduced in Chapter 3 along with its related experimental results and analysis. Second, we will focus on security enhanced approach based on the proposed non-cooperative iris recognition, including Chapter 4

and Chapter 5. The related biometric template protection methods and security enhance schemes are reviewed, analyzed and summarized in Chapter 4. Two cancelable template protection schemes based on the previous non-cooperative iris recognition approaches in Chapter 3 are proposed in Chapter 5. Finally, Chapter 6 draws some conclusions and future work.

2. RELATED WORKS OF NON-COOPERATION IRIS RECOGNITION

2.1 Traditional Iris Recognition

The iris (Figure 2.1) is the colorful ring of tissue that allows light to enter the interior of the eye. The iris is made up of connective tissue and has an intricate pattern of furrows, ridges and pigments spots. These patterns have proven to be unique from person to person in several large scale tests [17]. The iris is stable over long periods of time and it can be acquired in a non-contact manner. In addition, the universality of iris also makes it a good biometric trait for human positive identification.

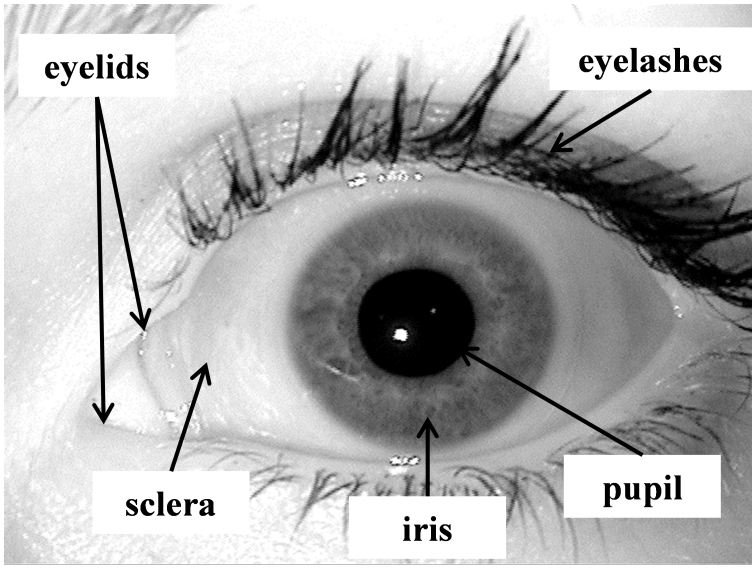


Fig. 2.1.: Iris image

Like other biometrics, iris recognition has both enrollment and recognition stages [28]. In the enrollment stage iris information is obtained in the following steps: image

acquisition, iris segmentation, feature extraction, template generation, and matching (Figure 2.2). The recognition process (Figure 2.3) includes acquisition, segmentation feature extraction and template generation, and template matching.

Fig. 2.2.: Iris enrollment process

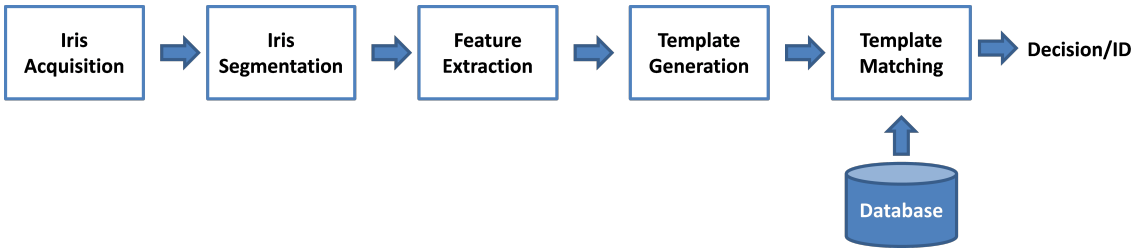


Fig. 2.3.: Iris recognition process

2.1.1 Iris Acquisition

The iris image acquisition acquires qualified images of eye region for further process. Iris images are usually acquired by a near-infrared (NIR) camera because NIR can reveal rich iris patterns even from iris with dark pigmentation [29]. For light color eyes, using visible lights can reveal enough features. Existing iris acquisition system can be divided into two types, depending on how much cooperativeness they acquired from the user. The first type is cooperative system which requires users to adjust their head position to acquire qualified images for the system [28, 30]. Most of the commercialized iris recognition systems are cooperative and the user may need to take several attempts to provide an acceptable image. The second type has fewer constraints in image acquisition. The system is trying to capture qualified iris image at a distance or while subjects are walking at a normal speed. Matey *et al.* have

designed less constrained iris recognition system, Iris On the Move (IOM), which can obtain iris images from people walking at normal speed through their system and then performs matching on the images that are obtained [31]. Fancourt *et al.* showed in [32] that it is possible to acquire qualified images at a distance up to 10 meters. Narayanswamy *et al.* [33] proposed a wavefront coded imaging technique to overcome the constraints of the lens and increase the iris imaging depth-of-field. Image quality measure and image restoration methods are also sometimes applied to ensure good image quality in less-cooperative situations [34].

2.1.2 Iris Segmentation

The iris segmentation module extracts iris patterns from the other eye parts (e.g. pupil, eyelids, and eyelashes) which are considered as noise [35]. In order to segment the iris part correctly, the pupillary boundary, the limbic boundary, the eyelids and eyelashes need to be detected.

Several typical segmentation algorithms have been proposed during the past two decades. The most commonly used method assumes that both limbic and pupillary boundaries are circles, which is referred as circular model based method. This type of methods looks for the circular pattern of iris and pupil and works well for frontal gazed images. Daugman [29] proposed modeling the pupil and iris as circles with integro-differential operators to detect the center and the radius by finding the maximum in the Gaussian blurred partial derivative with respect to radius, and center coordinates. Ma *et al.* developed a segmentation method by approximating the pupil centroid coordinates and applying Canny edge detection and Hough transform only in iris region determined by center of the pupil [36]. Similar implementations have been proposed in [37, 38].

However, the circular assumption is often not true in real life applications when a slight off-angle happens in the eyeball direction. The segmentation accuracy is not high in such situations. Some research proposed ellipse model based methods which

can mitigate the segmentation error in non-ideal situations. Zuo and Schmid [39] applied a rotated and translated ellipse based model with five parameters to fit the limbic and pupillary boundaries. Du *et al.* [34] proposed a video-based non-cooperative iris image segmentation scheme using a direct least-squares fitting of ellipses method to model the deformed pupil and limbic boundaries. Shapeless methods allow the iris and pupil boundaries to be segmented accurately even if it is not perfectly circular or ellipse. Daugman [2] proposed an active contour based segmentation method. This method describes the iris inner and outer boundaries in a snake graph. The thickness of this line represents the sharpness of the radial edge and the amplitude of the image represents the roundness of the snake. Shah and Ross proposed a geodesic active contours method to extract the iris from the surrounding structures [40]. This technique relies on the order of the Fourier series to approximate the inner and outer boundaries of the iris.

2.1.3 Iris Recognition

After the image has been acquired and segmented, it is important to extract stable and unique iris features and encode the features so that the unique features can be represented as templates. Once the image has been encoded it can then be compared to other encoded images. We categorize and discuss different types of iris recognition methods respectively.

2.1.3.1. Phase Information Based Approach

Daugman [29] proposed 2D Gabor wavelet on the polar image, and encoded the phase information according to the sign of the real and imaginary axis. All the current commercialized iris recognition systems are based on this algorithm.

$$h(Re, Im) = sgn(Re, Im) \iint I(\rho, \phi) \cdot e^{-i\omega(\theta_0 - \phi)} \cdot e^{-i(\frac{(r_0-\rho)^2}{\alpha^2} + \frac{(\theta_0-\phi)^2}{\beta^2})} \cdot \rho d\rho d\phi, \quad (2.1)$$

where $h(Re, Im)$ is the complex value, which is composed of binary real and imaginary values according to the sign of the 2D Gabor Wavelet output applied on the image, I, in the spatial domain. The wavelet sizes of the 2D Gabor Wavelet are α and β on the radial and angular axes, respectively, of log polar coordinates. The wavelet frequency on the angular axis is ω, which is 3 octaves inversely proportional to β. Hamming distance was used to measure the dissimilarity between any two iris templates.

Masek proposed a one dimensional Log-Gabor wavelet on the doubly dimensionless polar iris image to encode iris texture information [41]. The Log-Gabor Wavelet can be used as a band pass filter.

$$G(\omega) = e^{\frac{-log(\frac{\omega}{\omega_0})^2}{2log(\sigma)^2}}, \tag{2.2}$$

where σ is the filter bandwidth, and ω_0 is the center frequency of the filter. Log-Gabor filter is designed to remove the high and low frequency components inside the iris area. A one-dimensional FFT is used to find the frequency characteristics from $-\pi$ to π radians. The highest and lowest frequencies are removed by using the Log-Gabor Wavelet that is designed with the previously found parameters. The phase of each pixel of the polar image filtered with Log-Gabor Wavelet is found for encoding the iris patterns. A similar approach to Hamming Distance is used to calculate the similarity between two encoded iris images.

Hollingsworth *et al.* [42] found that not all of the bits in an iris code generated by Daugmans method [2, 29] are equally useful. They compared different regions in the iris area and found that the middle bands of the iris are more consistent than the inner bands. They also concluded that the inconsistencies are largely due to the coarse quantization of the phase response. Therefore they generated a Masking iris code bits corresponding to complex filter responses near the axes of the complex plane, which is shown to increase the recognition accuracy of Daugmans method in their experiments.

Velisavljevic [43] used the oriented separable wavelet transforms called directionlets to extract the iris features. Directionlets include separable 2-D basis functions

of the skewed asymmetric wavelets, which make use of asymmetry and directionality. Two low pass filters (the horizontal and vertical directions) and four directional high pass filters (0°,45°, 90°, and 135°) are applied to filter iris images. The matching score is calculated by a weighted Hamming distance score between two binary codes.

Miyazawa *et al.* [44] introduced a phase-correlation-based method for iris recognition in frequency domain using 2-D Discrete Fourier Transform (DFT). They found that two similar normalized iris images have a distinct sharp peak in the phase correlation function, which can be used as a good similarity measure for image matching.

Krichen *et al.* [45] found that phase based method can resist the effect of illumination variations. Therefore, it can be applied to degraded iris images captured in less cooperative situations. Instead of using DFT phase information, they construct the phase correlation function based on Gabor phase response for the reason that Gabor analysis can reflect the possibility of relating spatial information (pixel position) to the phase value extracted and can be used to extract information at different resolutions and orientations.

Thornton *et al.* [46] proposed an iris recognition technique that uses correlation filters designed in frequency domain. Their correlation filters are represented by several training images. A specific filter is designed for each iris class. The matching is done by performing cross-correlation between the test image and the filter impulse response. The resulting correlation output should contain a sharp peak if there exists a good match between the filter and image and no distinct peak if there is no match.

2.1.3.2. DCT Based Recognition Method

Monro *et al.* [47] proposed an iris feature extraction method based on differences of discrete cosine transform (DCT) coefficients of overlapped angular patches from normalized iris images. The segmented iris area is transformed and normalized into polar coordinate. Horizontally aligned overlapping patches in are then selected for feature extraction. The patches are averaged across width and windowed by a Hanning win-

dow. Finally, DCT is applied to the 1-D patch vector. The differences between the DCT coefficients of adjacent patch vectors are then calculated and a binary code is generated from their zero crossings. The Hamming Distance is used for matching.

2.1.3.3. Edge Map Based Iris Recognition Method

Wildes *et al.* [30] proposed use of a Laplacian pyramid to decompose the iris features for matching. The goodness of matching is measured by applying normalized correlation to the pair of filtered images.

Sudha *et al.* [48] proposed a new iris recognition approach based on the Hausdorff distance measure using edge map of iris images. They introduced a new measure, called local partial Hausdorff distance, which is computed between the binary edge maps of normalized iris images. This measure was proved effective in reflect dissimilarity between two images. Moreover, edge map requires less storage space while increases the recognition speed.

2.1.3.4. Blob Matching Based Approach

Sun *et al.* [49] proposed using moment-based iris blob matching to nd the spatial correspondences between the blocks in the input iris image and the enrolled one, and to quantitatively assess their similarity based on the number of matched block pairs. They also proposed to use cascaded classifiers to improve the accuracy, especially for noisy images.

2.1.3.5. Local Descriptor Based Approach

Zhu *et al.* [50] proposed a system to match iris based on the local scale invariant features; this method is called the scale invariant feature transform (SIFT) method. The advantage of this method is that it uses local feature therefore poor segmentation caused by occlusion or other noise doesnt affect the SIFT process as much.

Belcher and Du [34] proposed a region based SIFT approach for non-cooperative iris recognition which works for off-angle iris images. In their method, iris features are described without a polar transformation, affine transformation, or highly accurate segmentation and the feature point descriptors are scale and rotation invariant.

2.1.3.6. Quality Measure Incorporated Approach

Ma *et al.* [51] proposed an iris recognition method using local characteristics of iris texture variation applied on clear iris images. The proposed iris recognition method starts with image quality assessment and selection. A quality assessment algorithm is designed to select the highest quality portion of the iris patterns. Support Vector Machine is used as a classification mechanism.

Procenca and Alexandre [52] used frontal images of the iris taken in visible light spectrum. These images are non-ideal because there is more refection noise in the visible spectrum. Proenca *et al.* [53] observed that for non-ideal iris images, noise in one region decreases the iris recognition accuracy dramatically. The authors proposed dividing the normalized polar image into six regions, and applying a feature extraction algorithm on each region separately. Each iris has six biometric signatures, and the matching is performed on corresponding regions of two images separately. The dissimilarity values for six regions are combined to accept or reject the match. It is claimed that the proposed iris region division, regional feature extraction and matching method decreased the false rejection rate of the non-cooperative iris recognition algorithm more than 40%.

Vatsa *et al.* [54] applied a set of selected quality local enhancement algorithms to generate a single high-quality iris image. Then they used the 1D-Log Gabor Wavelets-based texture and topological feature extraction methods to extract the features from the enhanced image. The binary phase coding and Euler code based.

2.2 Non-cooperative Iris Recognition

Performing non-cooperative iris recognition is important for a number of potential tasks, such as video surveillance and watch list monitoring (identifying most wanted criminals/suspects). In addition, non-cooperative iris recognition systems can provide more convenience for cooperative users for identification. Non-cooperative iris recognition systems can effectively provide higher throughput therefore especially suited for applications in populated areas, such as airport, subway station, attractions, etc. However, non-cooperative iris recognition is still very challenging now due to the difficulty of locating the iris area accurately and describing the deformed feature properly. None of the methods reviewed in Section 2.1.3 is designed for non-cooperative iris recognition.

Some researchers have proposed off-angle iris segmentation algorithms. Daugman proposed the Fourier active contour approach to model the pupil and iris boundaries [2]. Shah and Ross [40] proposed a geodesic active contours method to extract the iris from the surrounding structures, which is proved to be effective in their WVU non-ideal dataset. Zuo and Schmid proposed a robust segmentation method based on image painting and contrast balancing [39]. He *et al.* proposed pulling and pushing model [55]. In [34], Du *et al.* proposed a video-based non-cooperative iris image segmentation scheme that uses a direct least-squares fitting of ellipses method to model the deformed pupil and limbic boundaries.

For non-frontal iris feature extraction, Daugman proposed using affine transform to correct the off-angle image and center the gaze [2]. However, this method is limited because the affine transform assumes the iris is planar, while actually it has some curvature. Schuckers *et al.* [56] proposed two methods to calculate angle of gaze: using Daugmans integro-differential operator and also an angular deformation calibration model. It needs an accurate estimate of the degree of off-angle and affine transformation. In [57], Belcher *et al.* proposed a regional based SIFT method for non-cooperative iris images. Iris features are described using local feature point descriptors without polar or affine transform. However, it describes the area around

a feature point using gradient information, which is not best suited for iris feature; therefore the accuracy is not high. Later, they introduced a new non-cooperative iris recognition method based on scale invariant Gabor descriptor [58]. This method can achieve good results for off-angle and partial iris images; however, it is slow in feature extraction. A faster feature point selection and description method is needed for real-time applications. The Gabor Descriptor method will be reviewed in Chapter 2.3 and the proposed multi-scale feature extraction and matching method for cooperative iris recognition will be presented in Chapter 3.

2.3 Review of Gabor Descriptor based Method for Non-cooperative Iris Recognition

The currently used iris recognition algorithm in most commercialized systems requires successful iris segmentation and global feature extraction on unwrapped iris templates, which are very challenging in non-cooperative situations. A possible alternative to deal with non-frontal looking and partial image is to locate several interest points in the partial iris region which are known as feature points. A properly designed local descriptor should be created for each feature points. The feature points are aligned and their descriptors are compared to generate a matching result.

The Gabor Descriptor method [58] does not require polar transformation, and can work with low resolution and off-angle iris images. In this method, the iris features are extracted using a Gabor descriptor. The feature extraction and comparison are scale-, shift-, rotation- and contrast-invariant. The Gabor wavelet is incorporated with scale-invariant feature transformation (SIFT) [57] to better extract the iris features. Both the phase and magnitude of the Gabor wavelet outputs were used in a novel way for local feature point description. The idea of Gabor Descriptor is the fundament of the new algorithm in this thesis; therefore we will give a brief review of Gabor Descriptor.

2.3.1 Preprocessing

In the preprocessing step, the iris area is segmented from the image (Figure 2.4). We used direct least square fitting of ellipse method to mathematically model the iris boundary:

$$F(\mathbf{a}, \mathbf{x}) = \mathbf{a} \cdot \mathbf{x} = ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{2.3}$$

where $\mathbf{a} = [a, b, c, d, e, f]^T$ and $\mathbf{x} = [x^2, xy, y^2, x, y, 1]^T$. Here we use $4ac - b^2 = 1$ as a constraint to improve the fitting efficiency and accuracy in high noise data. Then a window gradient-based method is applied to remove noise in the iris region [34].

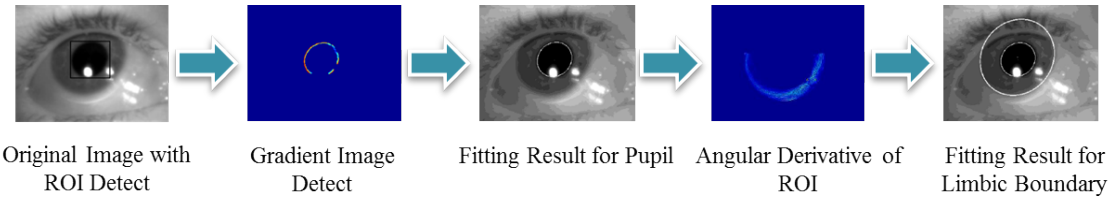


Fig. 2.4.: Non-cooperative iris segmentation steps

2.3.2 Feature Point Selection

The Difference of Gaussian (DoG) approach [57] is used to find the potential feature points which are invariant to scale, shift, rotation and contrast:

$$D(x, y, s) = G(x, y, s + 1) - G(x, y, s). \ (s = 0, 1, 2, 3) \tag{2.4}$$

G is the result of original image I(x,y) convoluted with Gaussian filter with different parameters:

$$G(x, y, s) = G_{\sigma_s} \cdot I(x, y). \tag{2.5}$$

Here,

$$G_\sigma(x, y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}, \tag{2.6}$$

$$g_{\sigma_s} = \sqrt{\sigma_0^2 + \sigma_s^2}, \tag{2.7}$$

where $\sigma_0 = 1.5\sqrt{2}$ and $\sigma_0 = 1.5(\sqrt{2})^s$.

The whole iris region is divided in to 720 sub-regions (Figure 2.5). For each sub-region, one extrema point at most is kept as the feature point. Lowe's 3-D quadratic method [59] and the Hessian matrix [60, 61] are used to test if a feature point is a stable point or not.

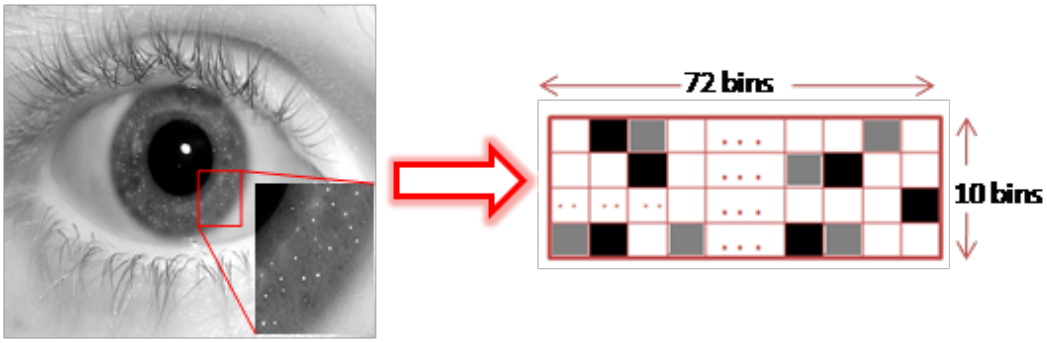


Fig. 2.5.: Sub-region map of feature points

2.3.3 Feature Point Description

Each stable feature point is then described using a vector with 64 elements, which is called a Gabor Descriptor. To create the descriptor for the feature point, a small window centered on this feature point is used for feature extraction. The window size is determined as:

$$W = \left\lfloor \sqrt{2} \cdot S_A \cdot \frac{N+1}{2} + 0.5 \right\rfloor, \tag{2.8}$$

where $S_A = (\sqrt{(x-x_p)^2 + (y-y_p)^2}) \cdot \frac{2\pi}{360} \cdot 5$ and N is the number of bins used to describe the relative position of a point to a feature point (here $N = 4$). S_A is the spatial extension of the frame around the feature point (x, y) in the angular direction, (x_p, y_p) is the coordinates of pupil center. S_A is used to normalize the window around that feature point and changes in size based on the distance between the feature point and pupil center.

A bank of 2-D Gabor filters is then used to extract the iris features. The Gabor filter in our research has the form:

$$G(x,y) = \frac{1}{2\pi\alpha\beta}\exp(-\pi(\frac{(x-x_0)^2}{\alpha^2} + \frac{(y-y_0)^2}{\beta^2})) \cdot \exp(i(\xi x + \nu y)), \tag{2.9}$$

where (x_0, y_0) is the center of the receptive field of the spatial domain, (ξ, ν) is the frequency of the filter, α, β are the standard deviations of the elliptical Gaussian along x and y directions.

The magnitude of the filtered area is Gaussian-weighted based on the spatial distance between each point and the feature point. The phase is divided into 4 areas. Finally, the weight is summed to form one of the 64 bins based on its spatial location referred to the feature point (4 x bins and 4 y bins) and phase quadratic (4 phase orientation bins). The 64 length Gabor Descriptor vector for each feature point is finally created by normalizing the cumulative weight to a unit vector (Figure 2.6). The details are shown below. The resulting 64 bin feature point descriptor is then normalized to a unit vector by dividing by the 2-norm of the descriptor.

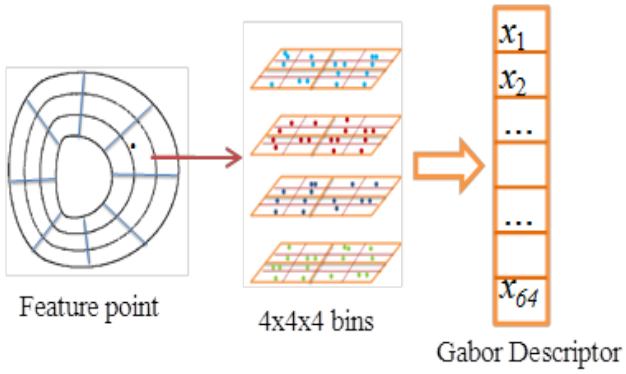


Fig. 2.6.: Feature point description

2.3.4 Feature Matching

To match two feature point maps, the average of the distance scores between all overlapping feature points is calculated and used as the matching score between two

feature point maps. To make the proposed method be tolerant of segmentation error and eye rotation, each feature point in a feature point map from image X, is compared to each feature point in the fifteen surrounding bins (two bins on either side and one bin above and below) in a feature point map from image Y, and the minimum average distance score is stored for the two feature point maps compared.

2.3.5 Discussion of Gabor Descriptor

Gabor Descriptor combines the Scale Invariant Feature Transform (SIFT) method and Gabor wavelet. SIFT method is proved to be effective in selecting interest point and tolerating affine transformation [57], which makes it a possible solution for non-cooperative or partial iris images. Gabor wavelet is proved to be suited for describing iris features [28]. It is reasonable that Gabor Descriptor achieves promising accuracy for non-cooperative iris images. However, there are still concerns and limitations of this method. First, feature points only from 1 scale are used in this method, however, in some situations, especially in low quality images, feature points are more easily to detect and more stable in higher scales. Second, feature points are detected and described within each sub-region, the overhead of filter convolutions is very high due to the large number of feature points and filters. This makes the feature point selection and description parts very slow. Third, there is no template protection scheme applied to the generated template, which could be a serious issue in real-life applications.

Based on the pros and cons of Gabor Descriptor, a newly designed feature point selection, description and matching algorithm is presented in Chapter 3.1. The proposed algorithm extracts more information from scale space and uses a multi-scale matching scheme. A series of approximations are applied to the feature point selection and description part to increase the speed. The experimental results on two databases are presented and compared to Gabor Descriptor and other methods in Chapter 3.2.

2.4 Local Descriptor

Existing local region descriptors such as SIFT [59] or GLOH [62] have been proved to be more effective and robust than global correlation methods under perspective and illumination changes. Moreover, for non-cooperative iris recognition, it is much easier to pair two set of local sparse points than align two deformable iris regions globally. The discrimination power of the local descriptor is highly correlated with the recognition accuracy, therefore how to properly design a descriptor is crucial.

2.4.1 SURF Descriptor

Speed Up Robust Features (SURF) presented by Bay *et al.* [63] has been proved an effective local descriptor and has been widely used in objects recognition and tracking. SURF descriptor describes each feature point by calculating the distribution of pixel intensities in a scale dependent neighborhood, which is very similar to SIFT [59]. However, SURF descriptor makes use of the integral image and the box-like Haar wavelet to decrease computing time.

The descriptor extraction can be divided into two steps. First, an orientation is assigned to each feature point to achieve rotation invariant. A circular SURF window is constructed first around each feature point. The size of the window is determined by the scale of the feature point. The response to Haar wavelet in both x and y directions are found for each pixel in the circular window. The orientation is calculated from the above Haar response and Gaussian weighted by the distance between each pixel and feature point. The orientation is estimated by the voting result of all pixels lying in the window to create a rotation invariant descriptor. This step is optional for some applications that do not require image rotation invariant very much. In this thesis, the orientation is used to pair two feature points in the multi-scale matching process.

The second step is to calculate the descriptor component. The aforementioned SURF window is divided into 4x4 sub-regions, and a 4-length-vector is calculated and extracted from the Haar response for each sub-region:

$$V_{sub} = [\sum dx, \sum dy, \sum |dx|, \sum |dy|], \tag{2.10}$$

where dx, dy are response to horizontal and vertical filter respectively. Finally a $64(4 \times 4 \times 4)$ length descriptor is generated for each feature point as SURF descriptor (Figure 2.7).

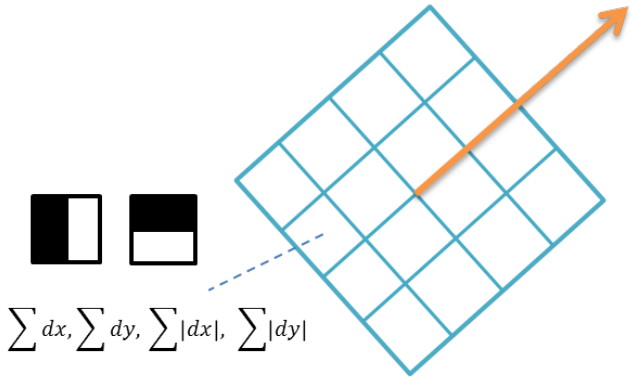


Fig. 2.7.: SURF descriptor

Unlike SIFT, the descriptor component calculation does not contain a spatial weighting scheme. All gradient attributed equally to the descriptor.

2.4.2 DAISY Descriptor

DAISY descriptor proposed by Tola *et al.* [64] are inspired by SIFT and GLOH but can be computer much faster. The efficiency is achieved by convolving orientation maps to computer each bin value of the descriptor using Gaussian. A global orientation map is pre-calculated and stored for each image. Thus there is no need to repeat the gradient histogram calculation during the descriptor generation.

For a given image I, H orientation maps G_i with the same size as I are computed first. H is the number of quantized orientations. The orientation map is computed using the image gradient norm: for each location $G_o(x, y)$ of the orientation map,

$$G_o(x, y) = max(\frac{\partial I}{\partial o}, 0). \tag{2.11}$$

Only the horizontal and vertical gradient $\frac{\partial I}{\partial x}$, $\frac{\partial I}{\partial y}$ need to be computer using kernel $[1, 0, -1]$ and $[1, 0, -1]^T$. other orientation norms can be directly derived using:

$$G_\theta = max(\cos\theta\frac{\partial I}{\partial x} + \sin\theta\frac{\partial I}{\partial y}, 0). \tag{2.12}$$

Each orientation map is then convolved with a set of Gaussian kernels H with different standard deviation σ. The Gaussian convolved maps can be computed very conveniently in a cascade way:

$$G_o^{\Sigma_2} = H^{\Sigma_2} \cdot G_o = H^{\Sigma} \cdot H^{\Sigma_1} \cdot G_o = H^{\Sigma} \cdot G_o^{\Sigma_1} \tag{2.13}$$

with $\Sigma = \sqrt{\Sigma_2^2 - \Sigma_1^2}$.

Based on the feature point location, a DAISY descriptor shown in Figure 2.8 is created. The size of the circle stands for the standard deviation of the convolved Gaussian kernel. the * sign is the location of feature point and the + sign is location of the central pixel of the sample region around each feature point. The overlapping regions guarantee the smooth transitions between different regions. The orientation is determined by the radial direction and quantized into one of the eight orientations of DAISY descriptor. (Figure 2.8)

2.4.3 Gabor Descriptor

2D Gabor wavelet has widely been used in feature extraction and object recognition. Daugman discovered that simple cells in the visual cortex of mammalian brains can be modeled by Gabor functions [28]. Thus, image analysis by the Gabor functions is similar to perception in the human visual system. Moreover, 2D Gabor filter has been proved very effective in iris feature extraction. Therefore, a filter bank

consisting of Gabor filters with various scales and rotations is created and applied in this research (Figure 2.9).

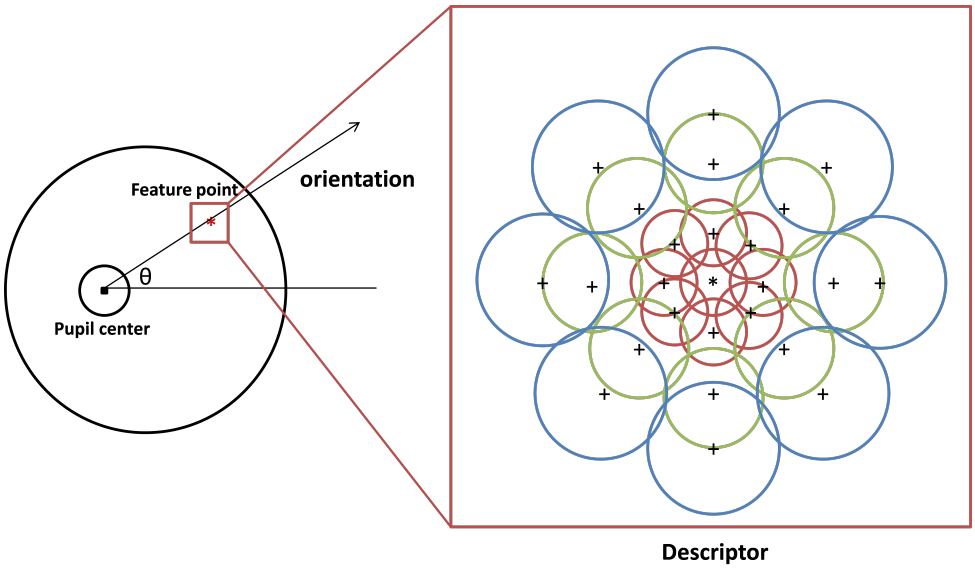


Fig. 2.8.: DAISY descriptor for non-cooperative iris

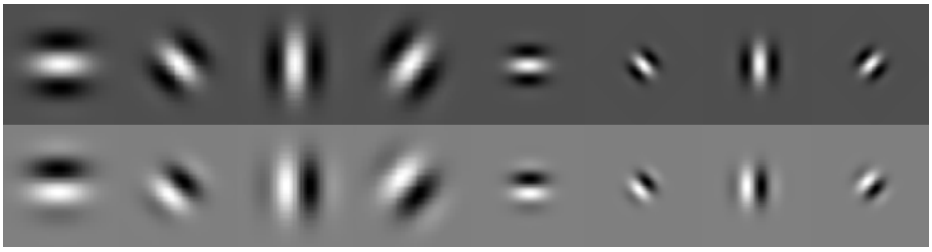


Fig. 2.9.: Examples of Gabor filters with different sizes and orientations.

By properly designing the parameter, a suitable Gabor filter bank is created for each detected feature point. The orientation of the Gabor filter is rotated in accordance with the radial direction of the feature point. A 4x4 neighborhood of the feature point is included for Gabor Descriptor (Figure 2.10).

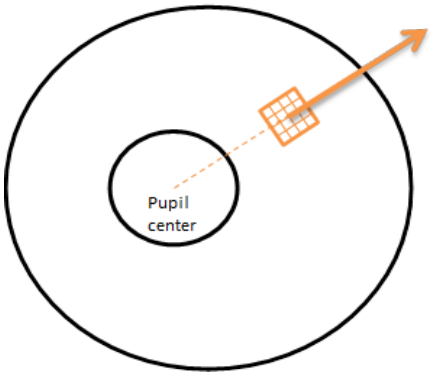


Fig. 2.10.: Gabor window and its 4x4 bins

3. SPEED-UP MULTI-STAGE NON-COOPERATIVE IRIS RECOGNITION

3.1 Speed-up Multi-Stage Non-cooperative Iris Recognition

Gabor Descriptor searches possible interest points within each sub-region. The DoG approach and hessian matrix based interest detection requires tons of convolution operations, which greatly increase the template generation time. Therefore only 3 different scales are used in Gabor Descriptor method, e.g. all the detect feature points are from only scale 2. The trade-off between the feature point completeness and running time may possibly reduce the discriminability of the generated Gabor Descriptor template. In this Chapter, a speed-up version of the Gabor Descriptor is introduced. Multi-scale feature extraction and matching scheme is applied to enhance the feature point repeatability increase the feature information.

3.1.1 Overview

The currently used iris recognition algorithm in most commercialized systems requires successful iris segmentation and global feature extraction on unwrapped iris templates, which are very challenging in non-cooperative situations. A possible alternative to deal with non-frontal looking and partial images is to locate several interest points in the partial iris region which are known as feature points. A properly designed local descriptor should be created for each feature point. The feature points are aligned and their descriptors are compared to generate a matching result.

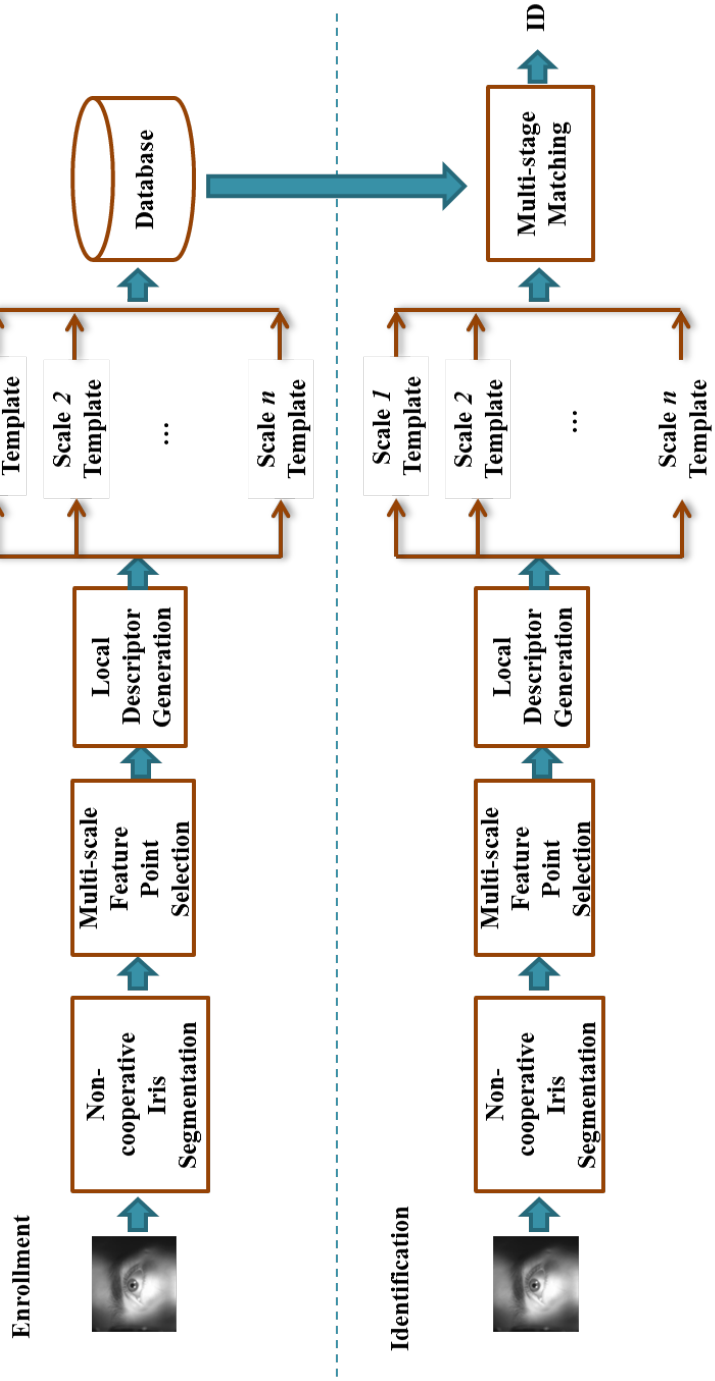


Fig. 3.1.: The diagram of the proposed multi-stage iris recognition approach

The flowchart of the proposed approach is shown in Figure 3.1. During the enrollment, the off-angle iris is segmented using our non-cooperative iris segmentation method. A multi-scale feature point selection algorithm is then directly applied to the segmented iris region. Local descriptor is generated based on the information around each feature point. Finally a multi-scale template is generated for each eye and stored in the database. During identification, the same segmentation and feature extraction methods are applied to the test image and a multi-scale template is generated. The generated template is compared with all templates enrolled in the database using a multi-scale matching algorithm to find the closest match. We will introduce the proposed approach step by step next.

3.1.2 Multi-scale Feature Point Selection

The filter convolution operation is very time-consuming. For example, an nxn filter convolution needs n^2 multiplications and $n^2 - 1$ additions, which leads to a $O(n^2)$ complexity. With the increase of filter size, the calculation time soars up. The integral image and box filter approximation similar to SURF method [63] are used here to speed up the filter convolution.

The integral image is computed rapidly from an input image and is used to speed up the calculation of any upright rectangular area. The integral image is generated by summing the entire pixel values between each pixel and the origin. For example, give an image I and a point (x, y), the value at (x, y) of the integral image I is calculated by the formula:

$$I_{\Sigma} = \sum_{i=0}^{i \leq x} \sum_{j=0}^{j \leq y} I(x, y). \tag{3.1}$$

The convolution of an image I with an $n \times n$ box filter with value f at point (x, y) can be implemented by only four operations using integral image I_{Σ}:

$$I_{conv}(x, y) = f \cdot ((A + D) - (B + C)), \tag{3.2}$$

where A, B, C, D is the value of the four corners of the convolved regions in integral image I_Σ: (Figure 3.2)

$$A = I_\Sigma(x - \left\lfloor \frac{n}{2} \right\rfloor, y - \left\lfloor \frac{n}{2} \right\rfloor) \tag{3.3}$$

$$B = I_\Sigma(x + \left\lfloor \frac{n}{2} \right\rfloor, y - \left\lfloor \frac{n}{2} \right\rfloor) \tag{3.4}$$

$$C = I_\Sigma(x - \left\lfloor \frac{n}{2} \right\rfloor, y + \left\lfloor \frac{n}{2} \right\rfloor) \tag{3.5}$$

$$D = I_\Sigma(x + \left\lfloor \frac{n}{2} \right\rfloor, y + \left\lfloor \frac{n}{2} \right\rfloor). \tag{3.6}$$

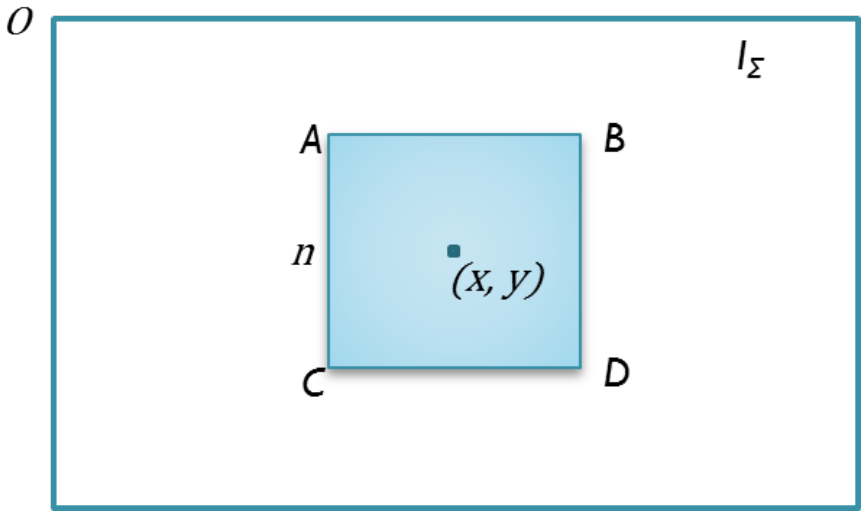


Fig. 3.2.: Filter convolution using integral image

To locate the interest points in multi-scale space, a scale-space needs to be created first. The traditional approach to constructing a scale-space is to change the image size and the Gaussian filter is repeatedly applied to smooth subsequent layers 3.3. This method requires a great many of convolutions and image resizing operations. To speed up this process, the Gaussian filter is approximated to a box filter only containing blocks of several values (Figure 3.5). Moreover, instead of changing the image size, the scale-space is created by convolving the unchanged image with a set of consecutively changed box filters (Figure 3.5). The filter size is decided by the scale of the points it detects 3.4:

$$filter_{size} = 3 \cdot (2^\sigma + 1). \tag{3.7}$$

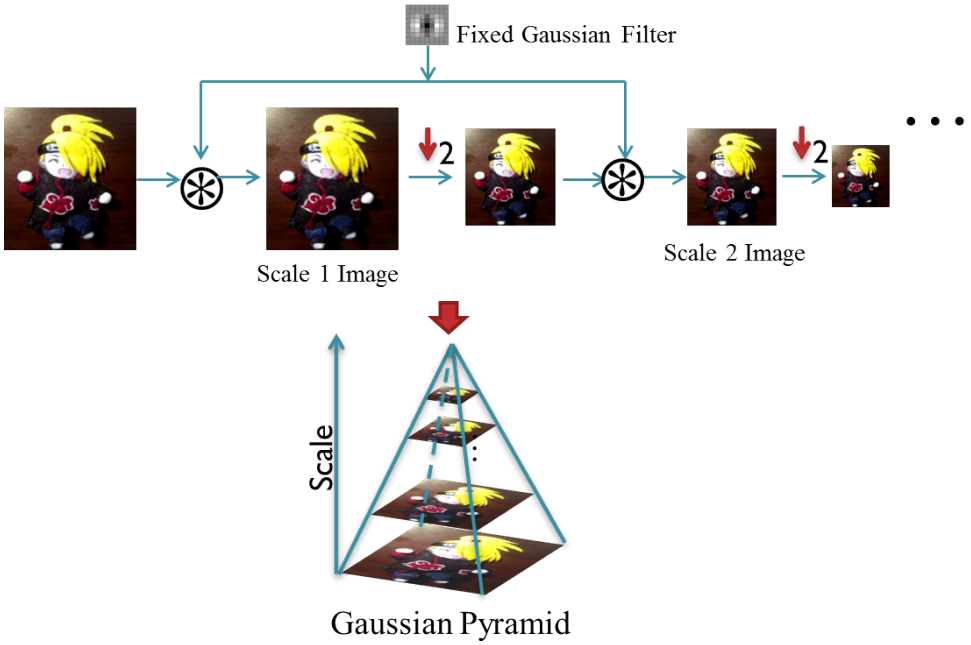


Fig. 3.3.: Construct scale space using Gaussian pyramid

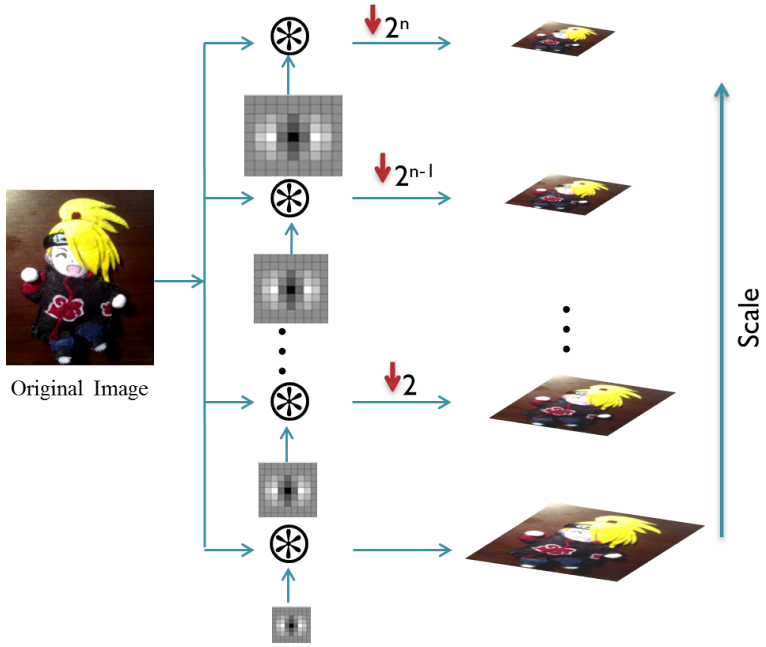


Fig. 3.4.: Construct scale space using filter pyramid

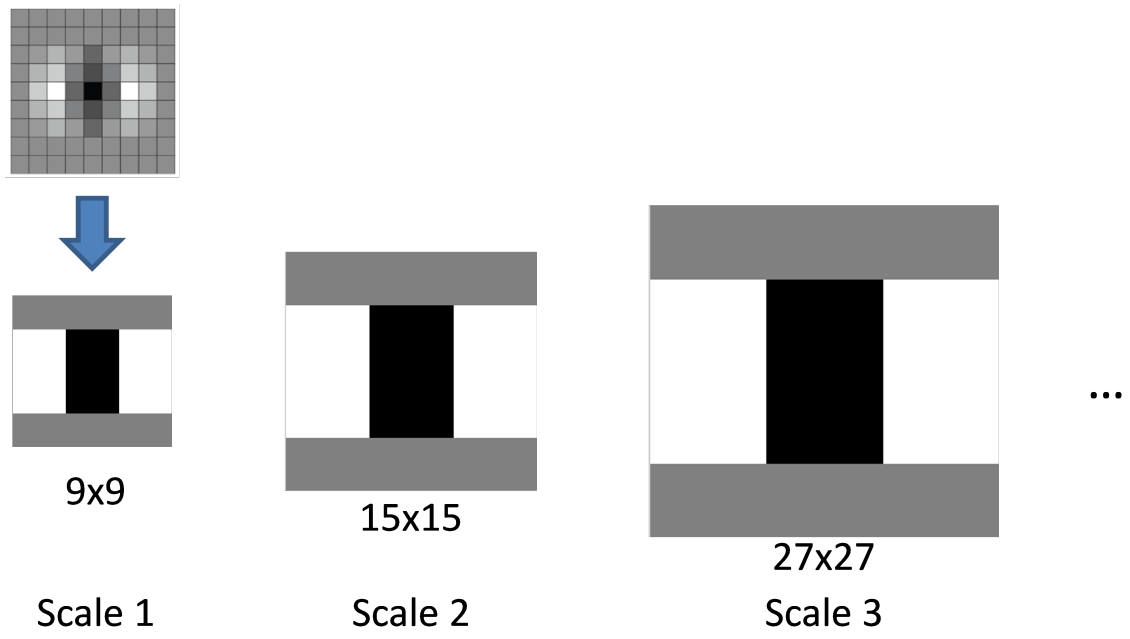


Fig. 3.5.: Approximated box filter structure

To locate the interest points, The Fast Hessian Detector [63] is used to find the potential feature points which are invariant to scale, shift, rotation and contrast. In order to accelerate this process, a similar set of box filters as in [63] is applied to approximate the Gaussian second order derivatives (Figure 3.6). For each point X = (x,y) in image, the Hessian matrix of X at scale becomes:

$$H(x,y,\sigma) = \begin{bmatrix} D_{xx}(x,y,\sigma) & D_{xy}(x,y,\sigma) \\ D_{xy}(x,y,\sigma) & D_{yy}(x,y,\sigma) \end{bmatrix}, \tag{3.8}$$

where D_{xx}, D_{yy}, D_{xy} are the convolutions of 3 approximated box filters with image in X. The points with positive hessian determinant value and greater than a threshold are selected as candidate feature points:

$$Det(H(x,y,\sigma)) = D_{xx}(x,y,\sigma) \cdot D_{yy}(x,y,\sigma) - 0.9^2 D_{xy}^2(x,y,\sigma). \tag{3.9}$$

All the candidate points are then compared to its 26 neighbors in a $3 \times 3 \times 3$ volume in scale space. The local maximum points are kept. (Figure 3.7)

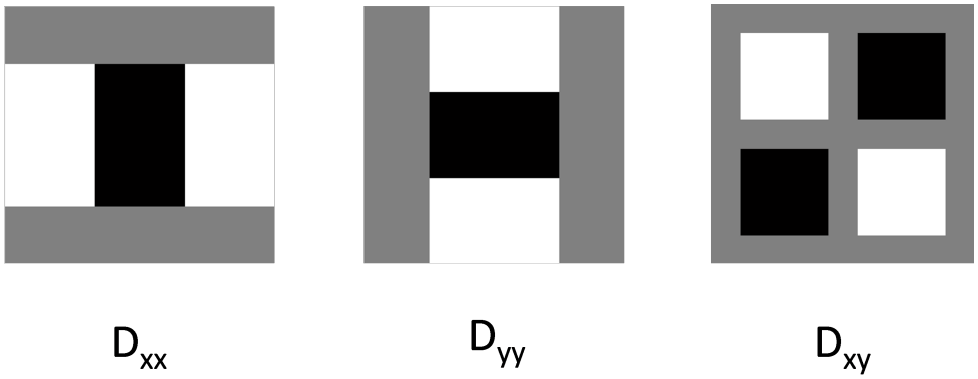


Fig. 3.6.: Approximated Gaussian filters for calculating Hessian matrix.

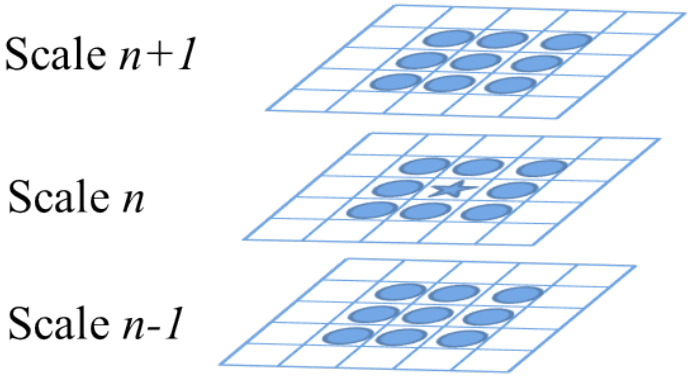


Fig. 3.7.: Local maximum point selection.

The final step is to interpolate the selected interest points in both spatial and scale to achieve sub-pixel accuracy. Brown's 3D quadratic method [65] is then used to interpolate each feature point in scale space:

$$D(\Delta\bar{x}) = D + \frac{\partial D^T}{\partial \bar{x}}\Delta\bar{x} + \frac{1}{2}(\Delta\bar{x})^T\frac{\partial^2 D}{\partial \bar{x}^2}\Delta\bar{x}, \tag{3.10}$$

where D and its derivatives are evaluated at the selected point and $\Delta\bar{x} = (\Delta x, \Delta y, \Delta\sigma)^T$ is the offset from this point. Taking the derivative of this function with respect to $\bar{x}$ and setting it equal to zero, we determine the extremum, $\Delta\bar{x}$, to be:

$$\Delta\widetilde{x} = -\frac{\partial^2 D^{-1}}{\partial \bar{x}^2}\cdot\frac{\partial D}{\partial \bar{x}}. \tag{3.11}$$

The refined location of the interest point is adjusted by $\Delta\widetilde{x}$ if any of $\Delta x, \Delta y, \Delta$ is greater than 0.5. The interpolation process is repeated until $\Delta\widetilde{x}$ is less than 0.5 in all the three directions.

For each sub-region divided in [58], at most one feature point is kept as the feature point. The one with the largest hessian determinant value is kept as the final feature point of this sub-region.

3.1.3 Multi-scale Local Descriptors

In [58], we developed the Gabor descriptor method. However, this method is slow and more importantly, detected feature points only from 1 scale are used in Gabor descriptor method, however, in some situations, especially in low quality images, feature points are more easily to detect and more stable in higher scales. In this research, we construct the scale space by subsequently convolving the image with a series of approximated box filters with different sizes. The convolution is done by applying the integral image, which greatly reduces the computation time. Within each scale, several feature points are located and described to generate a scale specified local descriptor. The local descriptors created at different scales compose the multi-scale descriptor for each iris (Figure 3.8).

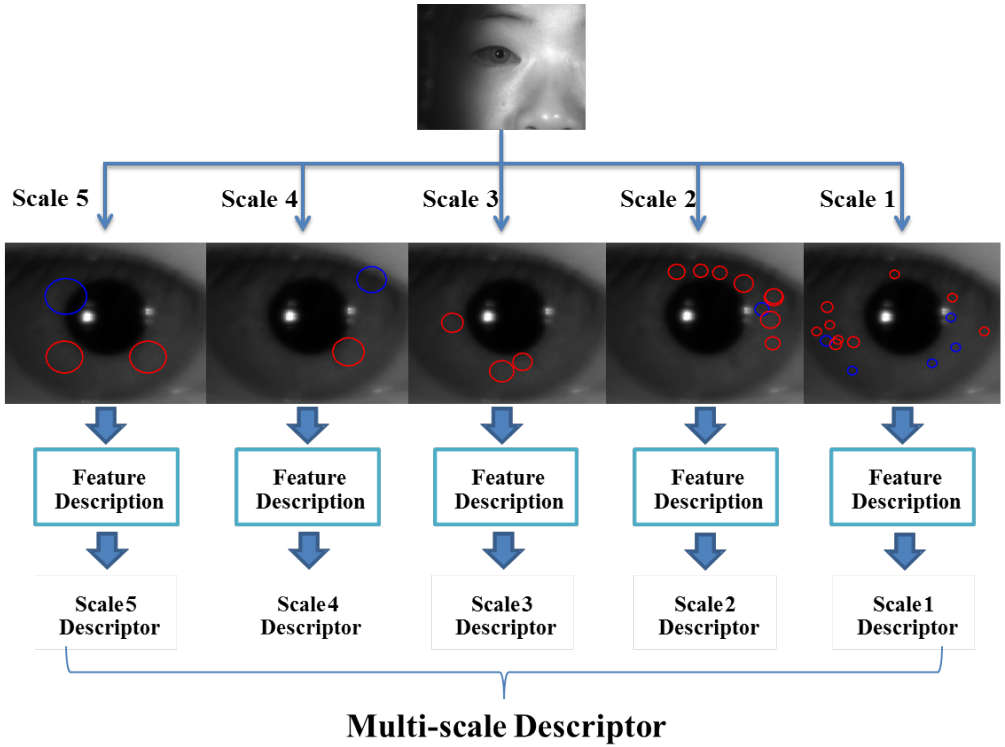


Fig. 3.8.: Multi-scale descriptor

Three kinds of local descriptors are selected or designed for non-cooperative iris recognition in this thesis: SURF descriptor, DAISY descriptor and Gabor Descriptor. The first two descriptors owe much of their strength to the use of gradient orientation histogram, which are relatively robust to distortion. SURF descriptor makes use of the Haar wavelet and the efficiency of integral image while DAISY descriptor takes much more correlated regions and orientations into consideration. In contrast, Gabor Descriptor relies on the response of the iris image to 2D-Gabor wavelet and created a phase based magnitude histogram. Their experimental results are compared in Chapter 3.2.

3.1.4 Feature Point Pairing and Multi-stage Matching

After generating local descriptor for each feature point, Two 10×72 feature maps is generated for the iris regions similar to Chapter 2.3. The two feature maps have 5 degree different to tolerate segmentation error and to enhance the robustness of the detected feature point location. While matching two irises, the feature points in two templates are paired based on the sub-region they belong to. To be tolerant of segmentation errors and eye rotation or dilation, during registration, each feature point is compared to its corresponding point and its neighbors in the other comparing template. Therefore multiple registrations are possible.

A multi-stage matching scheme is applied to each pair of compared templates after alignment (Figure 3.9).Feature points are paired by aligning two sub-region maps. At stage I matching, large scale points are paired and the paired point number is compared to a threshold. Only two irises with enough paired large scale points are kept to stage II matching, where the two multi-scale descriptors are compared to generate the final matching score.

We pair the feature points in two templates based on the sub-region they belong to. To be tolerant of segmentation errors and eye rotation or dilation, during registration,

each feature point is compared to its corresponding point and its neighbors in the other comparing template. Therefore multiple registrations are possible.

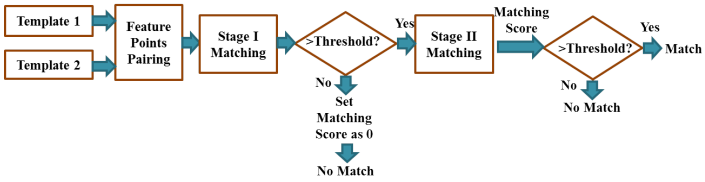


Fig. 3.9.: The proposed multi-stage matching scheme

Due to the stableness of the feature point extraction process, the feature points can be used as an important factor to determine iris class. In non-cooperative situations, it is common that iris images are not well focused, which may increase the difficulty of detecting detailed iris pattern at small scales. This will cause problems for feature points matching since the feature points detected at small scale may vary a lot. However, at large scales, we found that two irises from the same class remain a high stability in feature point locations. Therefore in the stage I matching, we separate the feature point pairs by their scale and check the feature points detected at large scales first(scale 3 to scale 5 in our experiment). If the number of repeated large scale feature points of all possible registrations is less than a threshold, these two irises are directly viewed as two different classes. In our research, the threshold is set to be 25% of the total large scale feature point number, which is proved to be very effective in reducing false acceptance without increasing too many false rejections. Two examples of feature points pairing at different scales are shown in Figure 3.10; we can see that these two images from the same iris maintain a high repeatability in feature point locations at large scales feature points (paired in red line) while the imposter iris is directly rejected after the stage I match since there are not enough detected feature points pairings. The size of the circle stands for scale and color of the circle stands for the sign of the trace of Hessian matrix.

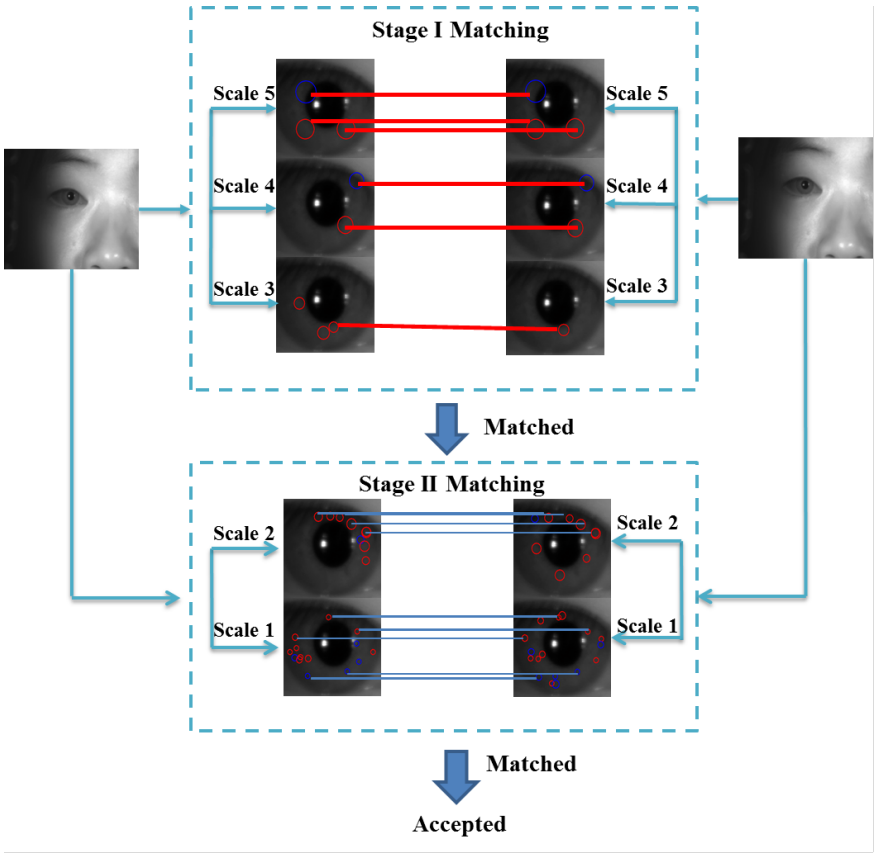
After the large scale feature point check in stage I matching, if the number of the paired large scale feature points is larger than the threshold, stage II matching

is followed. All feature points are paired based on their sub-region locations, scale, SURF orientation and the sign of the trace of Hessian matrix. Only if all the above information of two feature points is in accordance with each other, the pairing is valid. Two aligned irises are compared by checking the matching distance of the descriptors of all the overlapping feature points in stage II matching. For all possible registrations, the smallest average Euclidean distance of feature point matching pairs is the matching distance between the two images. The matching distance is used to further determine the iris class.

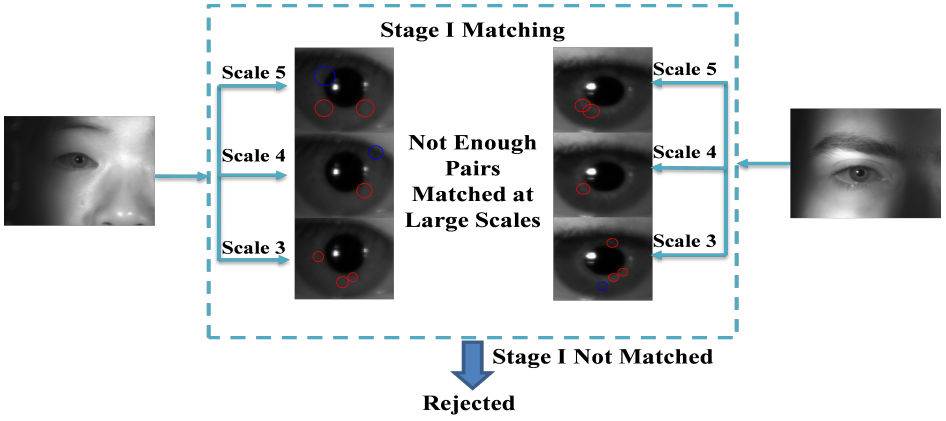
3.2 Experimental Results

3.2.1 Database

Two databases are used in the following experiments: IUPUI Remote Iris Image Database and ICE 2005 Database. The IUPUI Remote Iris Image Database was acquired at 10.3 feet from the camera to the subject using a MicroVista NIR camera with Fujinon zoom lens. The database includes 3690 remote iris images of 31 users in 6 directions (look left, look center, look right, look up-left, look up, look up-right) (Figure 3.11). 6 videos were captured for each subject with different scenarios: frontal look (1st video); reading from posters 15 feet from the subject and 5 feet behind the camera (2nd and 3rd videos; searching the wall to count the number of occurrences of a certain symbol (4th and 5th videos); and performing simple calculations using numbers posted on the ceiling (6th video). Each video was acquired at 30 frames per second with 1280x1024 resolutions. The average iris radius of the video images in the database is 95 pixels. During the image acquisition, subjects can move their heads and eyes freely to perform the tasks, which simulates a remote, non-cooperative situation, such as when a subject looks at flight times at an airport. In addition, the subjects can have their own emotions (smile etc.) during the acquisition process. Since there is no public available database particularly for non-cooperative iris recognition currently,



(a) A Genuine Match Example

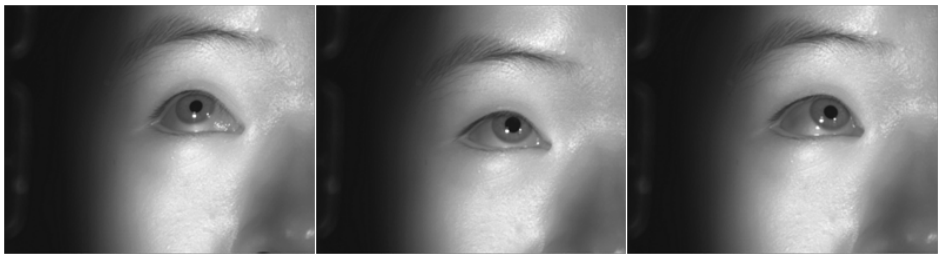


(b) An Imposter Match Example Match

Fig. 3.10.: Feature points pairing at different scales and multi-scale matching

we collected this dataset to measure the performance of our non-cooperative iris recognition methods.

(a) Look Left (b) Look Center (c) Look Right



(d) Look Up-Left (e) Look Up (f) Look Up-Right

Fig. 3.11.: IUPUI remote iris image database: multiple angles [58]

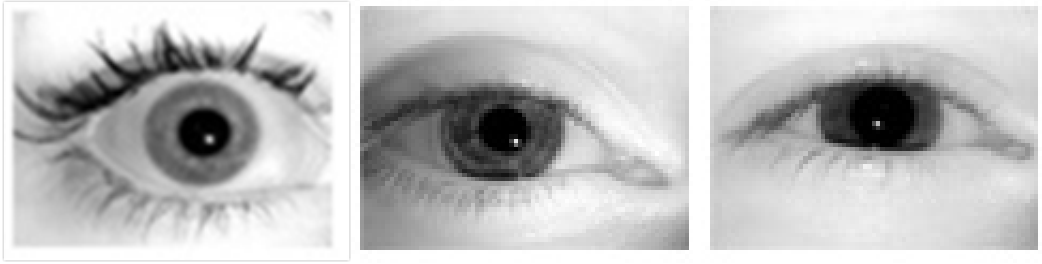


Fig. 3.12.: ICE 2005 database [66]

The ICE 2005 Database [66] from National Institute of Standards and Technology (NIST) consists mostly of frontal look eyes (Figure 3.12). It includes two sub-databases: a left iris image database with 1527 images from 120 subjects, and a right iris image database with 1426 images from 124 subjects. In this experiment, we used

the more challenging left eyes. The ICE 2005 Database is mainly used to measure the performance of our methods working in cooperative situation and to compare with other currently popularly used methods.

3.2.2 Experimental Results in Non-cooperative Situation

For the IUPUI remote iris image database, we used the ICE 2005 matching protocol in this experiment: each image is matched against all other images in the database. Therefore, all 3690 images were used in our experiment, comprising 6.8 million comparisons in the matching stage. We choose Gabor descriptor as the local descriptor to describe each feature point. We compare our proposed method with regional based SIFT method [57] and our previous Gabor descriptor method [58]. Figure 3.13 shows the comparison of receiver operating characteristic (ROC) curve between Gabor descriptor and our proposed method. The accuracy statistics of 3 methods are shown in Table 3.1. We can see that our proposed method achieves a 3.10% equal error rate (EER) and outperforms the other two previous non-cooperative iris recognition methods. The accuracy is increased due to the great reduction in false acceptance. The feature extraction of the proposed methods is 5 times speed up than Gabor descriptor method with increased recognition accuracy.

To ensure the accuracy, it will be important to have multiple enrollment images with different eye-looking angle in non-cooperative situation. Therefore, we also conduct a video based multiple iris fusion experiment. The identity is determined by a majority vote of all the recognized frames of each video. In this experiment, 10 images per eye were used from the first acquisition session for enrollment. They include the different off-angles (left, right, up-left, up-right, and up). The total number of enrollment images is 620 with 62 irises from 31 subjects. We automatically match the enrollment images with the video frames in the 5 videos for each person from the second acquisition session (the frontal look only video was excluded as they are all frontal images) for 30 subjects and 60 irises, altogether 298 videos. We achieve 100%

recognition accuracy (0% FAR at 0% FRR). The results show that 100% accuracy can be obtained using multiple enrollment images, video sequences of an iris, and fusion of matching results; even in a non-cooperative iris database.

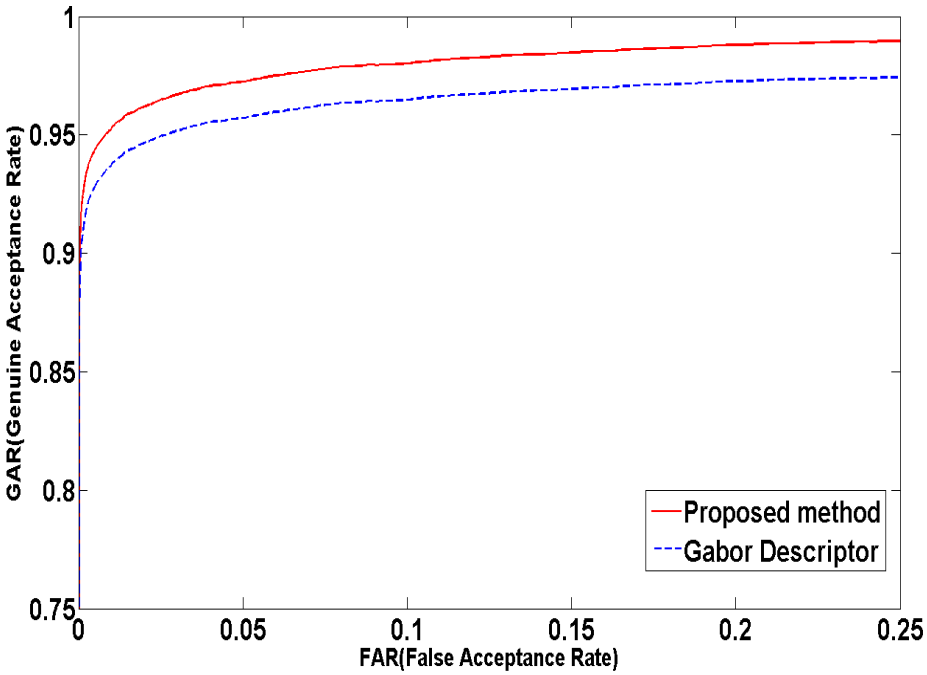


Fig. 3.13.: ROC curves comparison of IUPUI database

Table 3.1: Comparison of three methods using IUPUI non-cooperative database

Algorithm	EER	GAR at FAR = 0.1%	GAR at FAR = 0.01%
Regional SIFT [57]	5.88%	80.24%	67.63%
Gabor descriptor [58]	4.78%	89.66%	84.76%
Propose method	3.10%	92.20%	88.20%

3.2.3 Experimental Results in Cooperative Situation

We also measure the proposed algorithm in cooperative situation. We use the 1527 left eyes of ICE Database, which provides 1165101 comparisons. Gabor Descriptor is used for feature point description. The ROC curves of the all to all matching are shown in Figure 3.14. The proposed method outperforms our previous Gabor Descriptor based method. It is mainly due to the reason that the multi-scale matching algorithm can eliminate a lot of false matching at stage I matching. The proposed method is also compared with traditional method for frontal looking iris, 2D Gabor wavelet method [29] and 1D log-Gabor wavelet method [41] (Table 3.2). The same segmentation results are used for all the methods. The pupil and limbic boundaries are modeled as a circle, which is a simple and reasonable approximation of the pupil and limbic boundaries geometries for frontal looking eyes. We can see that our method can still achieve comparable results as the most accurate algorithms for cooperative iris recognition.

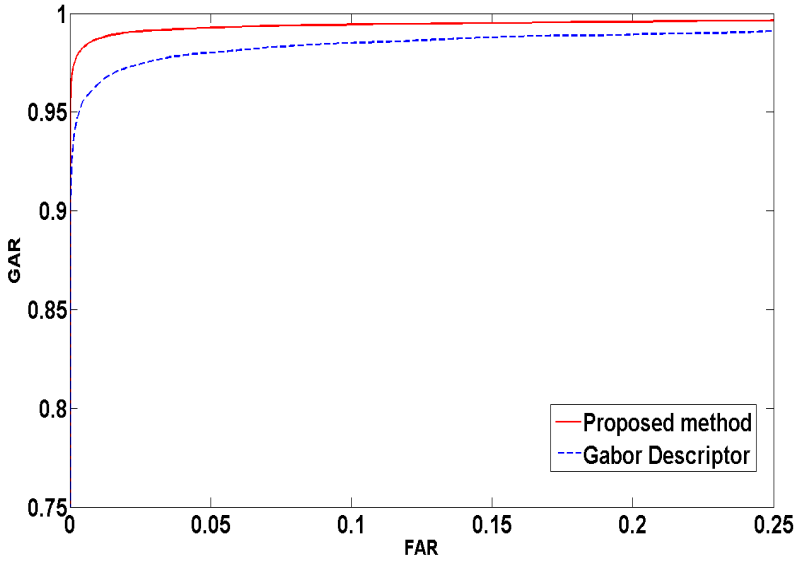


Fig. 3.14.: ROC curves comparison of ICE 2005 database

Table 3.2: Comparison of four methods using ICE 2005 left eyes

Algorithm	EER	GAR at FAR = 0.1%	GAR at FAR = 0.01%
2D Gabor [29]	1.26%	97.50%	96.29%
1D log-Gabor [41]	1.06%	97.39%	95.33%
Gabor Descriptor[58]	2.57%	93.16%	89.16%
Propose method	1.19%	97.20%	94.50%

To further justify the discriminability of our designed local descriptor, three different local descriptors (SURF, DAISY and Gabor) are applied to left eyes of ICE 2005 Database. The same set of feature points are detected and described using Gabor Descriptor, SURF Descriptor and DAISY Descriptor respectively. The comparison of ROC curves are shown in Figure 3.15. Obviously, Gabor Descriptor based local descriptor works better than the other two gradient based local descriptors. The main reason is because SURF and DAISY descriptor describe feature points using local gradient magnitude and angle information, whereas Gabor Descriptor encodes feature information around feature points using the magnitude and phase response of 2-D Gabor wavelets which is more capable of capturing iris feature characteristics. The detailed statistic results of the three local descriptors are listed in Table 3.3.

Table 3.3: Comparison of three descriptors using ICE left eyes

Descriptor	EER	GAR at FAR = 0.1%	GAR at FAR = 0.01%
Traditional SURF approach	5.99%	74.77%	61.03%
DAISY	9.41%	57.08%	40.53%
Proposed method	1.19%	97.20%	94.50%

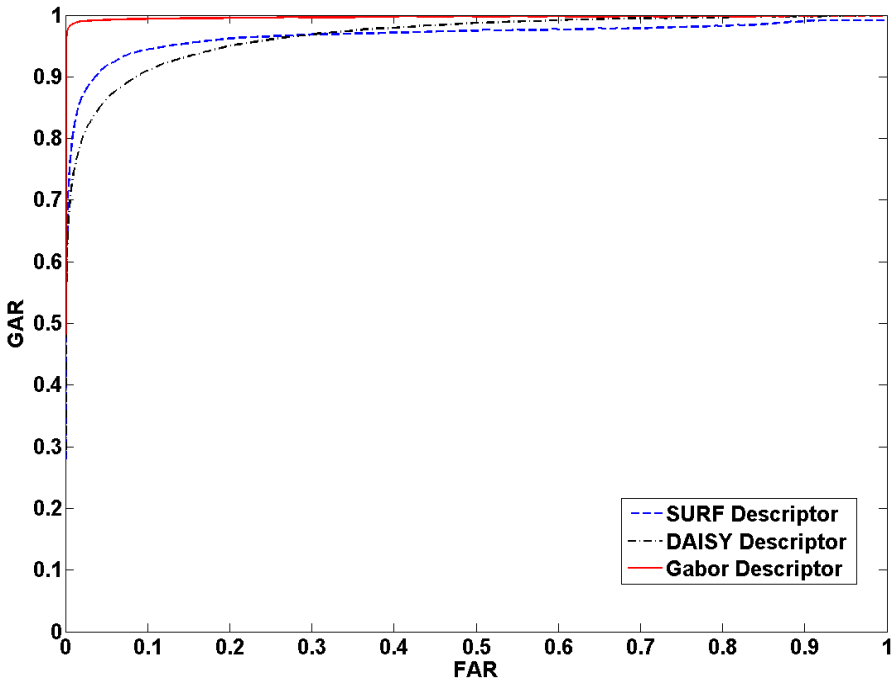


Fig. 3.15.: ROC curve comparison of three local descriptors

4. REVIEW OF BIOMETRIC TEMPLATE PROTECTION

In this chapter, Attacking on the biometric template is discussed and biometric template protection methods are categorized and analyzed.

Attack against the templates stored in database or during the matching process is considered to be one of the most potential threats to the traditional biometric systems. The intrusion into the template database may lead to serious consequences. Jain *et al.* [20] summarized three vulnerabilities related to attacks on templates: (i) an imposter can replace with a stolen template to gain unauthorized access. (ii) fake or replicated biometric patterns can be created to spoof the system. (iii) the stolen template can be replayed. Once the templates are stolen or tampered, it is possible that all the services relying on the same biometric pattern are in danger, which is known as the function creep [67]. Moreover, since biometric templates are usually highly connected to the user privacy and some of the personal information is sensitive, such as ethnic, gender, or the disease one is suffering from [68], privacy risks of the traditional biometric systems are of greater concern. The templates protection methods can mainly be categorized as the crypto and cancelable biometric approach. The first idea originated from the crypto community, combining biometrics with traditional standard cryptographic methods [69,70]. However, as we know, these algorithms (e.g. MD5) give totally different outputs even if their inputs are very close. In particular, these methods require extracting non-changing patterns from biometric data, which is often challenging. Therefore the design of a robust hashing algorithm to better tolerate the within-class variance of biometric templates while discriminating between-class distance is necessary. To solve these challenges, several types of methods have been proposed by the crypto community.

One popularly used method is biometric hardening or bioHashing [71–74]. The feature template is combined with user specific random information in order to be projected to a new representation. An error-tolerant discretization method is then used to quantize the feature description to reduce uncertainty. The projection acts like a linear transformation of the biometric pattern. It can protect the true template and ensure high security since the user specific random information can be generated using different keys, which ensures the revocability of the templates. Moreover, the introduction of user key can further increase the discriminability of the templates. However, external randomness needs to be stored in a smart card or a token, making it inconvenient in large scale applications. If the key is compromised, the scheme is insecure since the projection process is usually invertible. It is also noticeable that intrauser variation may reduce the stability of this scheme.

Key-binding [75–79] is another popular scheme in cryptosystem to protect the security of both biometric template and cryptographic key. This method depends on storing a helper data obtained by binding a key (which is independent of biometric template) with the biometric template [20]. Notice that the helper data should not reveal too much information about the key or biometric template. This scheme is considered to be non-invertible since it is computationally infeasible to decode the key or biometric template without knowing the biometric data. In [75], Juels and Wattenberg proposed the idea of fuzzy commitment which incorporates error correction code with local biometric features to tolerate the within-class variance. The method is proved to be effective in tolerating biometric data variations. However, it does not work well when substantial re-ordering happens in the biometric feature vector among different authentications, which is very common in biometric templates. Later, Juels and Sudan proposed the fuzzy vault [76] approach, which is an order-invariant version of fuzzy commitment. Note that this error correction based fuzzy scheme is first designed for a cryptosystem, but it is particularly suited for biometric data and biometric template protection. Therefore, it is often used in conjunction with other template protection methods, such as biometric hardening to achieve can-

celability [79]. However, current fuzzy vault scheme has some limitations; we will address this issue later in Chapter 5.

Another type of similar scheme is categorized as key-generation [80–84]. In contrast with the key-binding method, the helper data of key-generation scheme is only derived from the biometric traits and the cryptographic key is directly generated from the help data. The ideas of secure sketch and fuzzy extractor introduced by Dodis *et al.* [80] is an example design of key-generation cryptosystem. The secure sketch is the helper data extracted from the original biometric patterns which leaks limited information of the biometric data while the fuzzy extractor can generate cryptographic key from the biometric features. However, Simoens et al. [68] show that the attack on the fuzzy template protecting scheme is possible. In particular, it is possible for attacker to determine whether two documents are encrypted using the same biometric data. Even this does not mean that the biometric templates are compromised, but it is still a potential threat to user privacy. In addition, the stableness and diversity of the generated key cannot be easily achieved simultaneously [20].

The idea of cancelable biometrics [19] is proposed by Ratha *et al.*. This type of system implements cancelability by designing methods to transform the true signal and create alternatives for matching. These methods can be divided into two categories: one tries to mask the original patterns by mixing artificial texture or noise, which they called salting [85–88]. The other uses some non-invertible transformations to distort the original biometric patterns [89–92]. All these transformation functions are considered to be non-invertible since they are relying on some one-way functions which are easy to compute but hard to invert in polynomial time even if the attackers steal the transformed template and/or transformation key. Compare to other template protection methods, cancelable biometrics can preserve the biometric representation. The main concern of this type of methods focuses on whether the transform functions can preserve the discriminability of the biometric templates.

The comparison of the above four categories of methods are shown in Table 4.1 and all their advantages and disadvantages are listed in Table 4.2 [93].

Table 4.1: Comparison of different biometric template protection methods

	Stored entity	Preserve representation	Template stableness	Revocable
Biometric Hardening	Transformed template and key	No	Medium	Yes
Key-binding	Helper data	No	High	No
Key-generation	Helper data	No	Low	No
Cancelable Transform	Transformed template	Yes	High	Yes

Table 4.2: Summary of different biometric template protection methods

	Advantages	Disadvantages
Biometric Hardening	Easy to revoke and reissue Increase the discriminability	Invertible Original biometric can be recovered by the attacker if key is lost
Key-binding	Non-invertible High template stableness	Not cancelable Still leak some information High FRR
Key-generation	Non-invertible Directly generate key from biometric patterns	Stableness and diversity of the generated key can not be achieved simultaneously
Cancelable Transform	Keep representation Can be applied to raw data Easy to revoke and reissue Non-invertible	Reduce the discriminability Reduce accuracy

5. SECURE ENHANCED DESIGNS FOR NON-COOPERATION IRIS RECOGNITION

In this chapter, two secure enhanced designs for the non-cooperative iris recognition method in Chapter 3 are introduced to secure the iris template respectively: key incorporation based cancelable non-cooperative iris recognition and key-binding based cancelable non-cooperative iris recognition. The experimental results and related discussions are presented in Chapter 5.3.

5.1 Key Incorporation Based Cancelable Iris Recognition

In different from the traditional cancelable iris recognition methods which the key information is independent of the feature information. In this key incorporation scheme, we propose the partial-key information incorporation based cancelable iris recognition method. It is a non-invertible transformation. Figure 5.1 shows the system architecture. During Enrollment, a set of enrollment images is collected and preprocessed. The feature selection and description algorithms introduced in Chapter 3 are applied to each preprocessed iris pattern. A unique non-invertible transform method controlled by a random kernel is then carried out on each users Gabor Descriptor templates. Here we give a simple implementation of this random kernel: the user provides a key as a seed to a pseudo-random number generator which is used to create the random kernel. Thus, templates from the same user will have the same unique transformation. Finally, the transformed cancelable templates are stored in a database [94, 95].

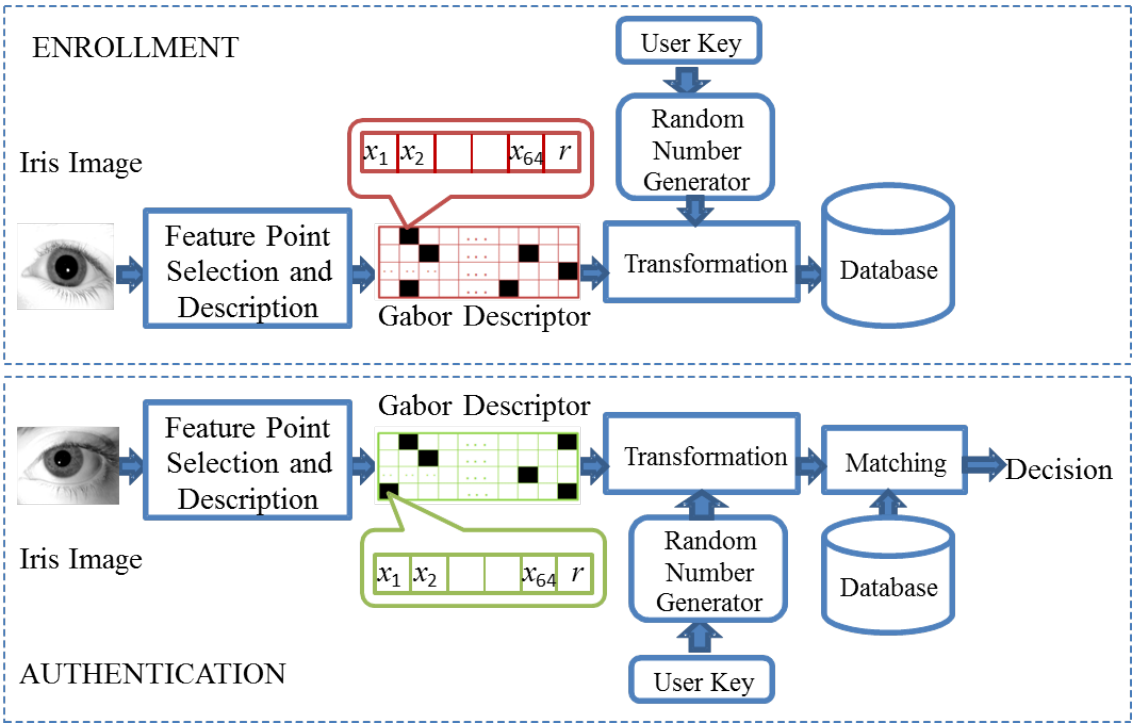


Fig. 5.1.: Proposed key incorporation cancelable scheme

During authentication (Figure 5.1), the user is asked to provide the user key to the system. The same feature selection and description algorithm is then applied to the preprocessed testing images. The user key produces the same seed to the pseudo-random number generator to realize a unique non-invertible transformation. Finally, two Gabor Descriptor templates are compared in a transformed domain to make a decision. Therefore if the transformed templates are compromised, the key can be reissued and the compromising would not affect the original templates.

5.1.1 Incorporating the Key Information

In this research, we used the fact that the ring information r can reflect key information and it is non-reversible. With this new feature information, the feature descriptor becomes a 65-length vector (64 bins plus the ring information). (an example is shown in Figure 5.2)

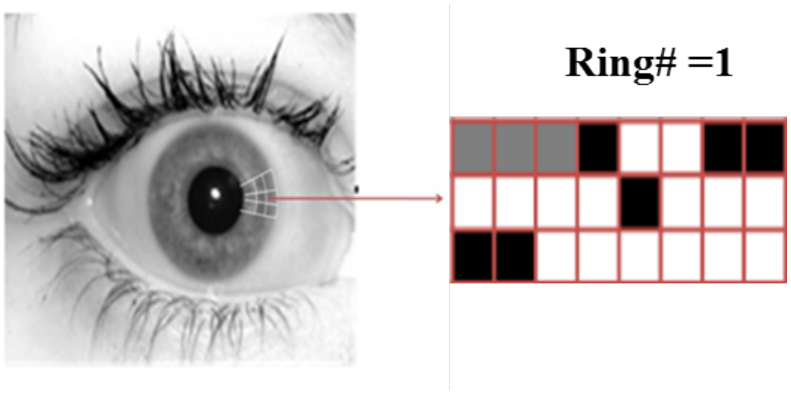


Fig. 5.2.: 65-length descriptor with ring information

The r information is actually the radial position in the sub-region map of each feature point. In order to enhance the template security and create cancelable template, a re-arrangement of the sub-region is needed. Before re-arrangement, the radial position of each feature point in sub-region map is recorded in r field added to the Gabor Descriptor. The re-arrangement is uniquely determined by a user key, which means a correct key provided should maintain the same re-arrangement. No matter how the transformation goes, the overlapping feature in original sub-region map should be still overlapping after re-arrangement. Thus, the recorded radial position of the overlapping feature point in both transformed templates should have the same r value. By checking the correspondence of the r values of each overlapping feature point in both test and enrolled templates, we can quickly get rid of the wrong user key situations. The key information is incorporated with the iris pattern and we do not directly compare the user key so there is less room for the attacker to get the key information. Moreover, the added r information will not leak the true template information because one cannot reverse the transform process only with the radial position in the sub-region map provided. Also, the key could not be fully recovered from the extracted key information.

5.1.2 Non-invertible Transformation

The transformation process is a non-invertible spatial transformation consisting of a random re-mapping of the 720 bins to shuffle the original location. Therefore theoretically 720! (over 10^{4200}) different transformations can be obtained. To be tolerant of segmentation error and provide redundancy, feature points located within a 3×5 neighborhood region are considered to be overlapping during matching. In our research, In order to make the re-mapping non-invertible, we only use part of the bins ($N < 720$) from the original templates which contains all the feature points so that the information for recognition will not be reduced. Therefore the true arrangement number is much less than the theoretical one. (For example, 100 valid feature points can get N!/(N-100)! different permutations). Even though, the number of possible arrangements is still enough to ensure a potential attacker has a negligible probability of guessing the arrangement of the original template using a brute-force attack.

In order to transform the original mapping arrangement, the user provides a random seed for a pseudo-random number generator. This seed may be generated by a physical hardware token that the user keeps in her possession; this provides a complex random seed in a secure manner. The results of the pseudo-random number generator are applied to a transformation process that re-maps each of the sub-regions from the original mapping arrangement into the newly transformed mapping. The transformation process re-maps the arrangement of the sub-regions, while leaving the contents of the 64-length descriptor in each sub-region unchanged from the original mapping. To realize the 720-bin random permutation, a 128-bit sequence is generated from each users pin or token as an input seed, as well as a set of encryption keys for the pseudo-random number generator. A one way hash encryption function or DES-based method can be used to map the input seed into 720 128-bit strings using the ANSI X9.17 pseudo-random number generator algorithm [96] below.

The 720 bit string sequence constitutes a unique random permutation applied to the original Gabor Descriptor templates. The pseudo-random number generator will produce the same numeric sequence when used with the same seed during a fu-

ture transformation process. This allows for subsequently generated iris mappings to undergo the same transformation, producing a consistently transformed mapping arrangement for matching. Even if the attacker gets the original template arrangement, that is just a part of the iris; the system can regenerate a new pin. The corresponding templates in the enrollment database should be deleted and the user should be re-enrolled in the database to achieve cancelability.

Algorithm 1 ANSI x9.17 pseudo-random number generator

For $i = 1 : m$

$x_i = E_k(I \oplus s)$;

$s = E_k(x_i \oplus s)$;

End

Return $(x_1, x_2, \ldots, x_m)$

I– initial value, s – input seed provided by user key, E_k – one-way encryption function controlled by encryption key extracted from user's pin or token.

5.1.3 Matching with a New Added Field

To match two feature point maps, the average of the distance scores between all overlapping feature points is calculated and used as the matching score between two feature point maps. To make the proposed method tolerant of segmentation error and eye rotation, each feature point in a feature point map from image X, is compared to each feature point in the fifteen surrounding bins (two bins on either side and one bin above and below) in a feature point map from image Y, and the minimum average distance score is stored for the two feature point maps compared.

In addition, we modified the Euclidean distance based matching algorithm by taking the transformation into consideration. For both enrolled and test images from a same user with the same key, the unique transformed mapping should be the same. During matching, any overlapping blocks of the transformed templates should also be overlapped in the original templates. Thus, we add a field which only records the

ring number of the bin to provide location information of this feature point. Before calculating the Euclidean distance, we check the feature point location information. If several blocks are found to be too far away, we view the two templates as being from different users and move on to the next comparison. The similarity (from 0 to 1) of two images X, Y is calculated as:

$$Sim(X,Y) = (X.r_1 == Y.r_1)\cdot(X.r_2 == Y.r_2)\cdot\cdots\cdot(X.r_m == Y.r_m)\cdot\sqrt{\sum_{i=1}^{64}(X_i - Y_i)^2}, \tag{5.1}$$

where $X.r_m$ and $Y.r_m$ are the ring location number of the mth overlapping block in both X and Y. An attacker cannot recover the original permutation with only the radius location information. Thus, with the added ring number, we can shorten our matching time and reduce the false acceptance rate greatly without compromising the security of the original templates.

In the matching process, there could be four possible scenarios: the two templates for matching could be from:

- *Same user and same key*: The two templates should be matched.
- *Same user and different keys*: The template matching distance would be high because the transformations are different and the two templates should not be matched.
- *Different users and same key*: The template matching distance would be high because iris patterns are different (i.e. Gabor Descriptors would be different so the distance will be high).
- *Different users and different keys*: The template matching distance would be high because both the iris patterns and the transformations are different. Under such a scenario, the false acceptance rate will be reduced dramatically.

5.2 Key-binding Based Cancelable Iris Recognition

To implement the key-binding based cancelable non-cooperative iris recognition, the fuzzy vault scheme is combined with the large scale feature point detection and description to enhance the iris template security. The high stability of the large scale point location from two irises from the same class can be utilized as the mutual information required by fuzzy vault scheme. However, the traditional fuzzy vault scheme has some limitations. Some of the limitations will be analyzed and addressed by the proposed design in this Chapter 5.2.1. The proposed fuzzy vault implementation for biometric template protection is introduced in Chapter 5.2.2.

5.2.1 Fuzzy Vault Scheme

Fuzzy vault scheme [76] proposed by Juels and Wattenberg is a cryptographic construction specifically suited for biometrics. A player Alice may place a secret key k in a fuzzy vault and lock it use a set of elements from a universal field. In order to retrieve the secret key k from the locked fuzzy vault, another player Bob has to present his set of elements which is substantially overlapped with that of Alice to unlock the fuzzy vault. Thus, fuzzy stands for the fuzziness of the set of elements held by every player. The player who wants to unlock the vault and obtain the secret key does not need to present the exactly same set with the one used for locking. A small portion of fuzziness and variation is allowed.

Due to the variations of signal acquisition situations, the acquired biometric signals from the same user are not exactly identical every time. The fuzziness of the biometric signal can be utilized to construct a fuzzy vault, which is a typical design of key-binding biometric template. The generated key-binding template (vault) is referred as helper data in the key-binding based biometric template security protection schemes. The helper data is the only information stored in the database, which leaks negligible information of the true biometric template. In this way, the privacy and security of users biometric template is secured.

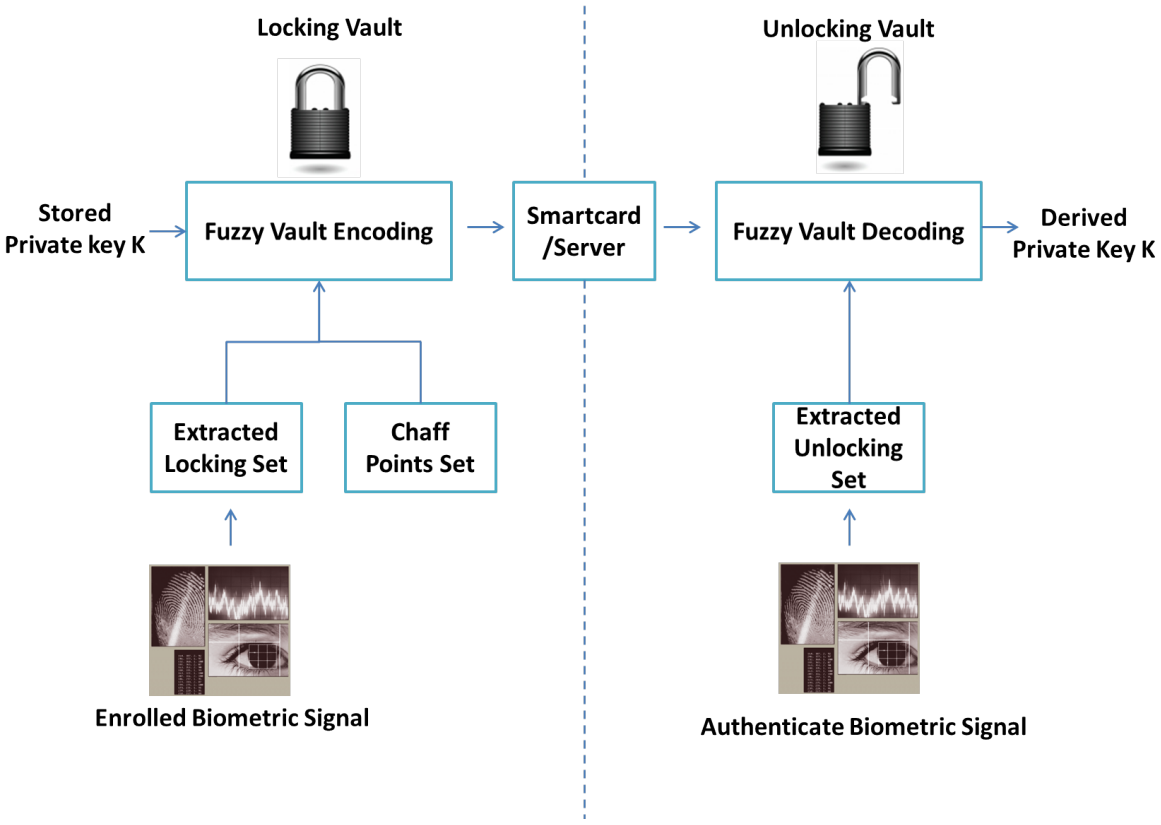


Fig. 5.3.: Traditional fuzzy vault scheme

A formal description of the fuzzy vault scheme is shown in Figure 5.3. During the fuzzy vault locking, a locking set

$$B_{lock} = \{B_{lock\_1}, B_{lock\_2}, \ldots, B_{lock\_n}\} \tag{5.2}$$

is extracted from the enrolled biometric signal. A private key K is stored in the vault in the following way: assuming K is a 128-bit AES key; the key is then divided into 16 8-bit binary strings. A polynomial P of degree 15 is constructed using the previous 16 binary number as its coefficients. The locking set B_{lock} is evaluated using the polynomial and a genuine locking set

$$T = \{(B_{lock\_1}, P(B_{lock\_1})), (B_{lock\_2}, P(B_{lock\_2})), \ldots, (B_{lock\_n}, P(B_{lock\_n})\} \tag{5.3}$$

is generated. In order to hide the genuine set T, a chaff point set

$$C = \{(C_1, Q(C_1)), (C_2, Q(C_2)), \ldots, (C_m, Q(C_m))\} \tag{5.4}$$

is created and mixed into the genuine set T. Note that any point $(C_i, Q(C_i))$ in C should not lie on polynomial P, e.g., $Q(C_i) \neq P(C_i)$ for any $i \in [1, m]$. A redundancy set R is created based on B_{lock} to correct errors when unlocking the vault. Error correction code, such as Reed-Solomon code is applied to encode the locking set B_{lock} and generate the redundancy code set R. Finally, a fuzzy vault $V = \{T, R, C\}$ is locked and stored in a smartcard or server. Note that the created vault V is supposed to reveal only very little information of either the private key or biometric signal, therefore it can protect the privacy and security of both private key and biometric information of user.

During the fuzzy lock unlocking, an unlocking set

$$B_{unlock} = \{B_{unlock\_1}, B_{unlock\_2}, \ldots, B_{unlock\_n}\} \tag{5.5}$$

is extracted from the authentication biometric signal. The B_{unlock} is corrected using the redundancy code set R generated when locking the vault. If the authentication biometric signal is similar enough to the enrolled one, the error correction code should be able to correct all the error bits and recover the exactly same set as B_{lock}. It is now very easy to separate the genuine set T and chaff point set C from the vault V. After is successfully recovered from V, the polynomial P is derived using Lagrange interpolation. Suppose $T = \{(x_1, y_1), (x_2, y_2), , (x_n, y_n)\}$ is obtained from the error correction, for instance, RS decoding, $P(x)$ is interpolated as follows:

$$P(x) = \frac{f(x)}{(x - x_1)f^{'}(x_1)}y_1 + \frac{f(x)}{(x - x_2)f^{'}(x_2)}y_2 + \ldots + \frac{f(x)}{(x - x_n)f^{'}(x_n)}y_n, \tag{5.6}$$

where

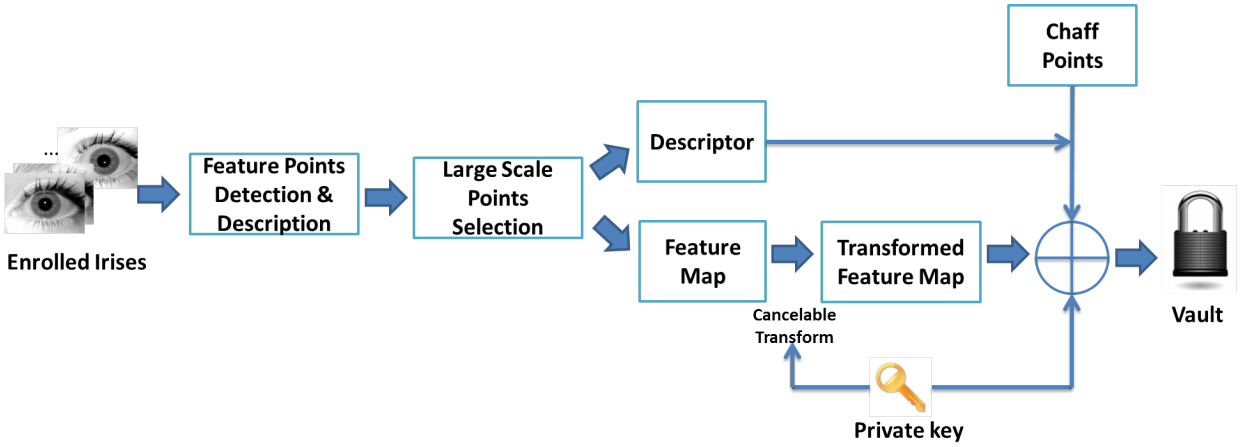
$$f(x) = (x - x_1)(x - x_2)\ldots(x - x_n), \tag{5.7}$$

and $f^{'}(x)$ is the derivative of $f(x)$. Finally the private key K is recovered by concatenating the coefficient of $P(x)$. Obviously, fuzzy vault can be used to protect a private key for encryption usage. In the other hand, the match of the derived key with the stored key indicates the match of biometric signal, therefore fuzzy vault can also be used as a template secured biometric authentication scheme.

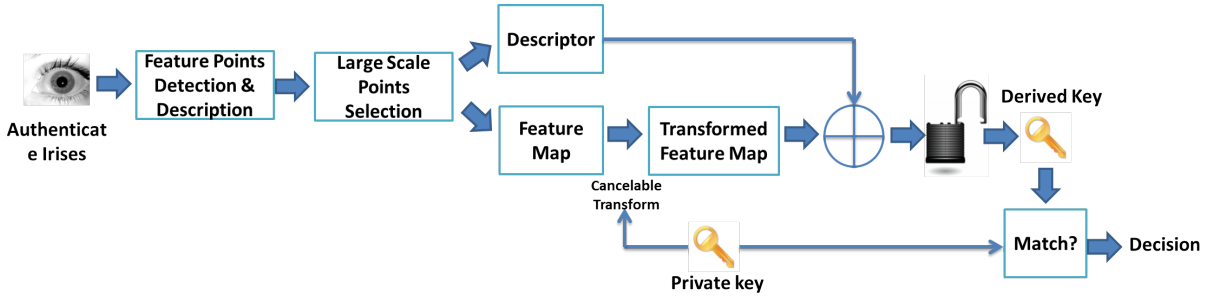
However, the above scheme has some limitations if directly applied to biometric system. First of all, the scheme is not cancelable or revocable, e.g., if the biometric template is stolen, there is no easy way to revoke the obsolete vault and reissue a new one like password. That will lead to severe consequence in real-life applications. Second, the application of error correction requires the whole encoding and decoding process implementing in Galois Field (GF). It is very challenging to transform the biometric template into a stable binary template with low bit error rate. Moreover, the more variation between the enrolled template and the authenticate template, the more bits is needed for the error correction redundancy code, which makes the encoding and decoding process very time-consuming. The proposed design in this chapter will mainly address the above two concerns.

5.2.2 Proposed Fuzzy Vault Design for Non-Cooperative Iris Recognition

The proposed fuzzy vault design in this thesis makes use of the stableness of the large scale feature points detected among irises from the same class in Chapter 3. The positions of the matched feature point pairs are used as the genuine set T mentioned in Chapter 5.2.1. The descriptor of the corresponding feature point is compared to the enrolled template to determine whether it is an enrolled point. No error correction code is needed for this scheme. There is also no need to store the private key in the server. Instead, the private key is held by user himself/herself as a smartcard or token, which eliminates the danger of being hacked in the server. The flowchart of the proposed design is shown in Figure 5.4. We will discuss the vault locking and vault unlocking process separately next.



(a) Vault Locking



(b) Vault Unlocking

Fig. 5.4.: Flowchart of proposed design

Locking the vault

During the vault locking process (Figure 5.4a), several iris images from each subject are selected as the enrollment/training images. Feature points are located and described using the method introduced in Chapter 3. The more stable large scale points are picked out as the candidate locking set. In this design, only feature points with scale 3 or higher are selected. The corresponding 10×72 feature map and local descriptor are generated.

To make the locking set cancelable, a user specified external randomness (a unique user key or token) is added to the scheme. A 128-bit private key is used to re-arrange the feature map. Each sub-regions of the original 10×72 feature map is re-mapped to a new position on the 256×256 transformed feature map (Figure 5.5).

To realize the transform, the unique 128-bit private key is input into a pseudo-random number generator as a random seed. The results of the pseudo-random number generator are applied to a transformation process that re-maps each of the sub-regions from the original mapping arrangement into the newly transformed mapping. The transformation process re-maps the arrangement of the sub-regions, while leaving the contents of the local descriptor in each sub-region unchanged from the original mapping. A one way hash encryption function or DES-based method can be used to map the input seed into 720 128-bit strings using the ANSI X9.17 pseudo-random number generator algorithm [93]. The 720 bit string sequence constitutes a unique random permutation applied to the original feature map. The pseudo-random number generator will produce the same numeric sequence when used with the same seed during a future transformation process. This allows for subsequently generated iris mappings to undergo the same transformation, producing a consistently transformed mapping arrangement for matching. if the attacker gets the original template arrangement, the system can regenerate a new pin. The corresponding templates in the enrollment database should be deleted and the user should be re-enrolled in the database to achieve cancelability.

To lock the vault, the 128-bit private key is divided into 8 16-bit binary strings and each string is a coefficient of the 8-degree polynomial P. The coordinates of each feature point on the transformed feature map are used as the input of the polynomial. The x, y coordinates (0-255) of each feature point is converted into an 8-bit binary code and the two binary code are concatenated as $x \mid y$. The concatenated coordinates are evaluated by the polynomial P. The genuine set T is created as $T = \{(B_1, P(B_1)), (B_2, P(B_2)), , B_n, P(B_n)\}$ where $B_i = x_i \mid y_i$, $\mid$ stands for concatenation and n is the number of enrolled feature points.

To hide the genuine set, a set of chaff points C is added to the genuine set T and the number of chaff points is from 1 to 64816 (65536 - 720), depending on the required security strength (Figure 5.5). A fake descriptor for each chaff point is randomly generated and stored along with the true descriptor as D. The fuzzy vault $V = \{T, C, M, D\}$ is finally locked, where T is the genuine set, C is the chaff point set, M is the 256×256 transformed feature map and D is the corresponding descriptor.

Unlocking the vault

During the vault unlocking (Figure 5.4b), each user presents both his/her iris pattern and a unique private key to the system. The same feature points detection and description process is applied to each authenticate iris. The large scale feature points are located and a corresponding feature map and a descriptor set. The generated feature map is remapped to a 256×256 feature map by the unique private key using the same algorithm as the vault locking. The transformed feature map is compared with the enrolled feature map M in the vault to find the all the overlapping feature points. Only those overlapping pairs with close descriptors are considered to be a valid hit. The similarity of two feature points is determined by the Euclidean distance of their related descriptors. The x, y coordinates of the hit points are concatenated and the genuine set T of the vault is recognized. Lagrange interpolation in Chapter 5.2.1 is applied to the genuine set T to recover the polynomial P and the locked private key is derived. The match of the derived private key with the user key indicates a successful authentication.

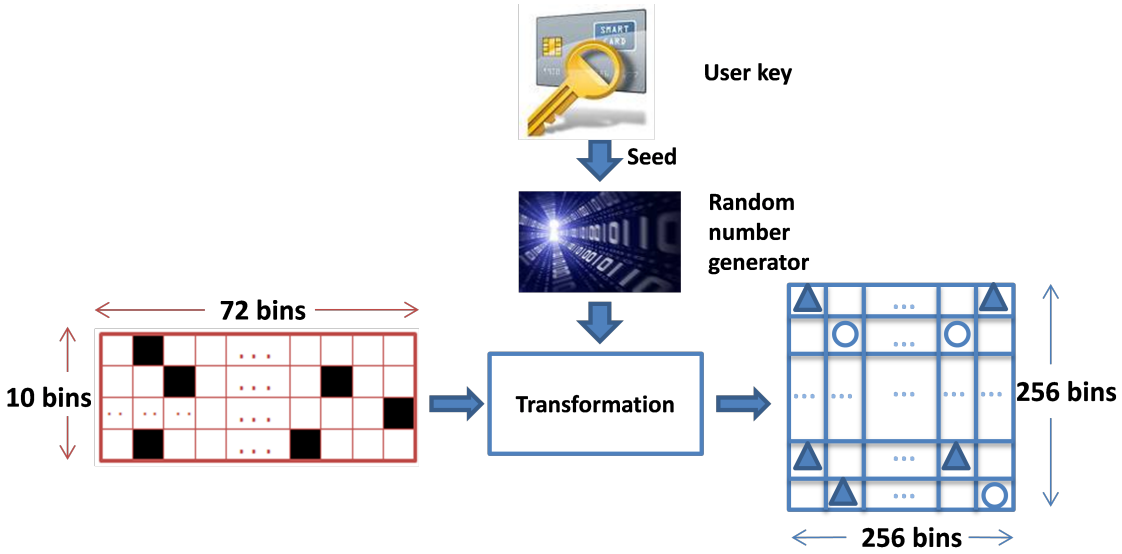


Fig. 5.5.: User specified transformation.

During the authentication, there could be four scenarios:

- *The same user with the correct private key*: The access is valid if there are enough hit points to unlock the vault.
- *The same user with incorrect private key*: The access should be denied since the wrong key will lead to a wrong transformation. The derived key will not be able to match with the user key due to the lack of hit points.
- *Different users with correct private key*: The access should be denied since the small similarity between the two irises will lead to a completely wrong unlocking set, which derives a mismatched key.
- *Different users with incorrect key*: The access should be denied because neither the iris pattern nor the user specified transformation is matched therefore the probability of the match of the derived key from a completely wrong unlocking and the incorrect user key is negligible.

5.3 Experimental Results

5.3.1 Experimental Results for Key Incorporation Cancelable Scheme

For experiment 1, we use the 1527 left eyes of ICE Database, which provides 1165101 comparisons. In order to show the performance of our method in general situations, we randomly assign a unique key to each user and apply random transformations to the biometrics templates every time and we do this 10 times, which means we revoke the old key and re-issue a new key 10 times. We first apply the traditional method without key information incorporated to the 10 transformed datasets, The 10 ROC curves using traditional Gabor Descriptor are shown in Figure 5.6a, the results using key information incorporated cancelable approach are shown in Figure 5.6b. The EERs comparisons of the 10 random experiments are listed in Figure 5.6c, we can see that the recognition accuracy has been dramatically improved.

Table 5.1 compares using 2-D Gabor wavelet matching, 1-D Log-Gabor matching, our Gabor Descriptor and the proposed cancelable method results on annular iris images of the ICE database. To be comparable, all the methods use the same segmentation method and frontal-look images. It is shown that our original Gabor Descriptor method can achieve accuracy close to the traditional 2-D Gabor wavelet method and 1-D Log-Gabor method. Our proposed cancelable method can effectively reduce the FAR to achieve 0.001 EER. Moreover, our methods can work well in non-cooperative situations (off-angle eyes). Most of the eyes from different classes are directly rejected during the stored ring number checking process; therefore high accuracy is reasonable.

We also compare the proposed key incorporated cancelable iris recognition method with the matching results from top iris recognition companies/groups who participated in ICE in 2005 [66]. (Table 5.2) Our key incorporated cancelable method can achieve better results than the best team, at the same time achieving cancelability.

For experiment 2, IUPUI database is used to measure the performance of the key incorporation cancelable scheme for non-cooperative situation. We used the ICE 2005 matching protocol in this experiment: each image is matched against all other images in the database. Therefore, all 3690 images were used in our experiment, comprising 6.8 million comparisons in the matching stage. Our own non-cooperative segmentation algorithm was used to automatically obtain the iris region. Similar to experiments on ICE database, we randomly assign a unique key to each user and apply random transformations controlled by the user key to the iris templates of each user. The 10 times results of our traditional method without key information incorporated are shown in Figure 5.7a. We then use the proposed cancelable approach to test the 10 trials; the results are shown in Figure 5.7b, where we can see that our result is very steady and promising. Figure 5.7c shows the 10 EERs (Equal Error Rates) comparison: Our Gabor Descriptor result for IUPUI database is 5.24% while the average EER of our 10 times experiment using proposed method is 0.3965%.This shows that the proposed method does not change the genuine matching results, but greatly increases the matching distance of imposters.

Table 5.3 compares the results of using the two traditional cooperative iris recognition algorithms, 2-D Gabor wavelet matching [29] and 1-D Log-Gabor matching [41], with our Gabor Descriptor [58] and the proposed cancelable method on the centered eyes from our IUPUI remote database. The proposed method result is the average result of 10 times experiments. To make the comparison result reasonable, we only use the 610 frontal-look images (cooperative situation) and use the same segmentation outputs. Our Gabor Descriptor method results are comparable to the results achieved using traditional matching algorithms and our proposed cancelable method can effectively reduce FAR, which improves the accuracy.

All the above experiments using the key incorporation cancelable method achieve very promising results, which is reasonable because we pre-assigned totally random keys to different users. The key variation will result in totally different transformations which will be detected by our matching algorithm with ring information

examination. Therefore, nearly all the false acceptance cases are excluded because they cannot pass the ring number check mechanism. One thing to point out here is, our scheme is not a direct and simple combination of key check and iris comparisons, but incorporates the key information into the biometric templates. We do not directly compare the user key but extract the key information from the iris templates and quickly exclude imposters. The extracted key information reveals just a small part of information of both transformation key and original biometric template, which makes it impossible for attackers to recover the true information. In such a way, we can better protect the user key and achieve high accuracy, as well as reducing the matching time.

From our experimental results, we can see that our method effectively obtains cancelability while reducing the FAR greatly and thus improving the recognition accuracy. Most of the false acceptances are rejected due to our transformation checking mechanism by comparing the stored ring number before matching. The unique cancelable transformation actually provides more information for identity verification. Moreover, the non-invertible transformation is carried out on descriptor templates without changing or ruining the original feature information. Thus, the added transformation greatly increases the recognition accuracy.

5.3.2 Experimental Results for Key-binding Cancelable Scheme

For the key-binding cancelable scheme, left eyes of ICE 2005 database is used to measure the proposed fuzzy vault design in Chapter 5.2.2. There are 119 subjects altogether and the first iris image of each subject is encoded to form the vault. A unique 128 bit private key is assigned to each subject to conduct the cancelable transformation and is used to create the vault locking polynomial as well.

To measure the False Rejection Rate (FRR), all other irises from the each subject are through the same feature detection and extraction process. The remapped template is generated and compare with the one locked in the vault. The genuine

set is determined by checking the distance between the overlapping feature points from the vault. Lagrange interpolation is applied to the derived genuine set and to reconstruct the polynomial whose coefficients are concatenated as the 128 private key. The matching of the derived private key with the assigned key indicates a genuine acceptance. For different polynomial degrees, the Genuine Acceptance Rate (GAR) is shown in Figure 5.8. For all the 16180 intra-class matching, we achieve a 95.94% GAR at degree 4, which means a 4.06% FRR. As the polynomial degree goes up, more hit points are needed to unlock the vault therefore the increase of FRR is reasonable. However, even for degree 8, we still achieve an 89% GAR. The results are promising compared to other fuzzy vault implementations [78, 97–99].

To measure the corresponding False Acceptance Rate (FAR), we try to unlock the vault using the irises which are not the same class as the enrolled one, which consists 1150448 inter-class matches. Theoretically, with the increase of polynomial degree, the FAR should be reduced since the possibility that an inter-class pair of iris contains enough hit points to unlock the vault at high polynomial degree is negligible. For all polynomial degrees from 4 to 8, none of these inter-class tests can unlock the vault. Hence the FAR of the proposed scheme is 0, which is very promising.

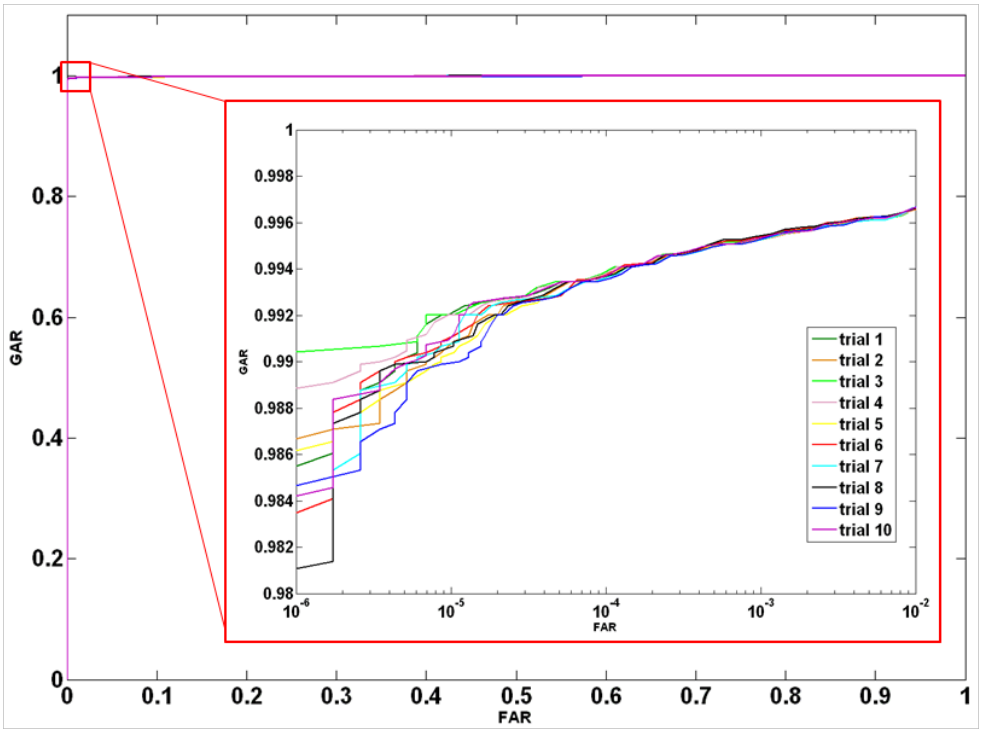
We can also measure the security of our fuzzy vault system quantitatively. Assume that an attacker tries to unlock the vault by separating the genuine set from the chaff points set using brutal force attack. To unlock a vault of polynomial degree 8, at least 8 genuine points needs to be correctly located. The vault has altogether 65536 points and we suppose each iris has 20 feature points at high scale which is the average case, therefore the possibility of a successful brutal attack is $C(20, 8)/C(65536, 8) \approx 1.5 \times 10^{-29}$. In another word, it will take an average of 6.7×10^{28} trials for an attacker to crack the vault, which corresponds to a computational time of more than 7×10^{11} years for a 3.0 GHz computer if we assume each trial takes even only one evaluation.

Table 5.1: Comparison of different matching algorithms for ICE 2005 left eyes

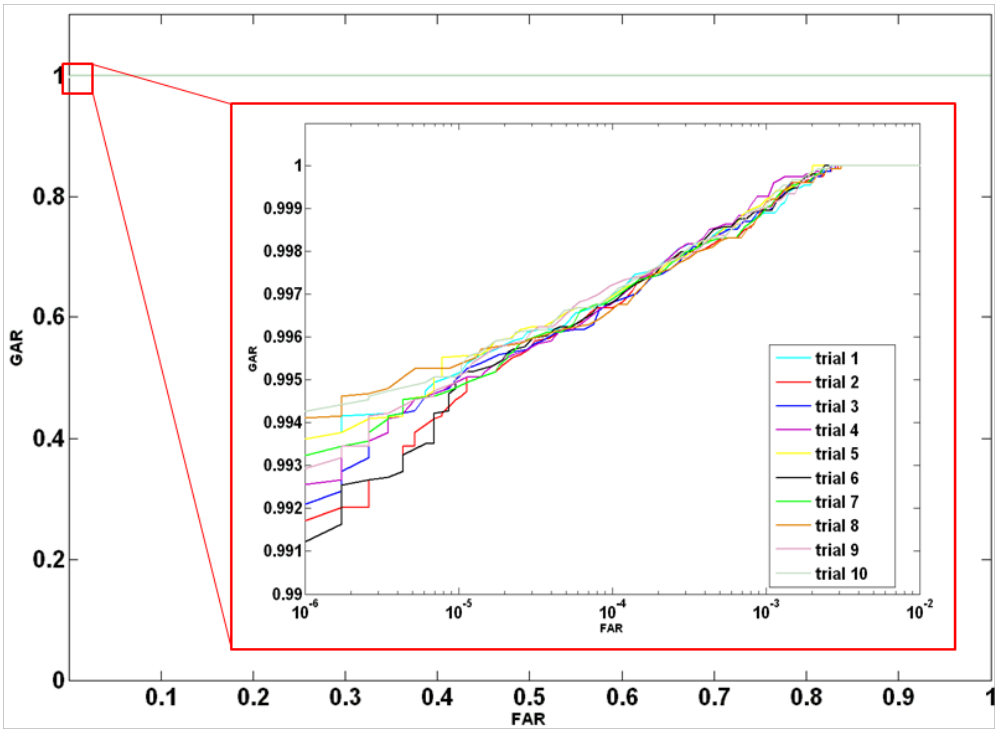
Algorithm	Images #	EER	GAR at FAR = 0.1%	GAR at FAR = 0.01%
2-D Gabor	1527	1.26%	97.50%	96.29%
1-D Log-Gabor	1527	1.06%	97.39%	95.33%
Gabor Descriptor	1527	2.57%	93.16%	89.16%
The proposed cancelable approach(average result from 10 trials)	1527	0.10%	99.85%	99.62%

Table 5.2: Comparison of our method and others results

Group name	Database used	GAR at FAR = 0.1%	GAR at FAR = 0.01%
SAGEM [13]	ICE database left eyes (1527 images)	99.1%	98.9%
IritchD[13]	ICE database left eyes (1527 images)	99.2%	98.6%
CMU[13]	ICE database left eyes (1527 images)	99.1%	98.2%
CAM2(Daugman's method) [13]	ICE database left eyes (1527 images)	98.9%	98.6%
Proposed cancelable method	ICE database left eyes (1527 images)	99.8%	99.6%

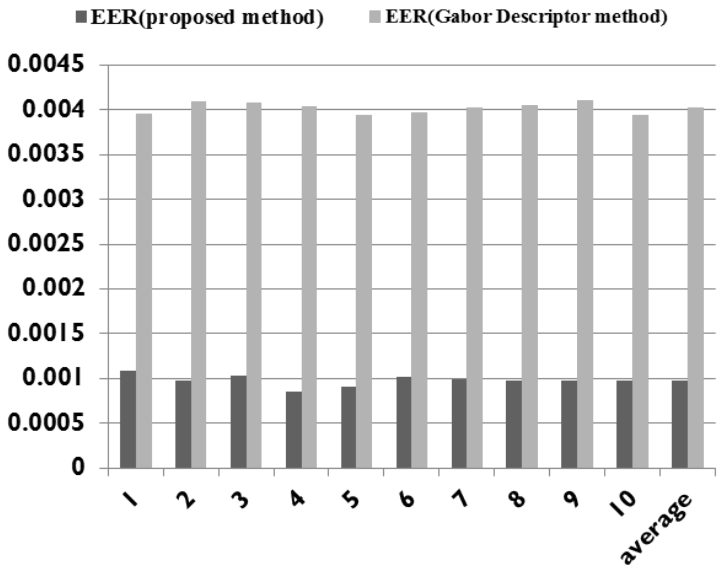


(a) ROC Curves of 10 Trials using the Gabor Descriptor Method (ICE)



(b) ROC Curves of 10 Trials Using Proposed Method (ICE)

Fig. 5.6.: Result of experiments on ICE 2005 database (ICE database left eyes)

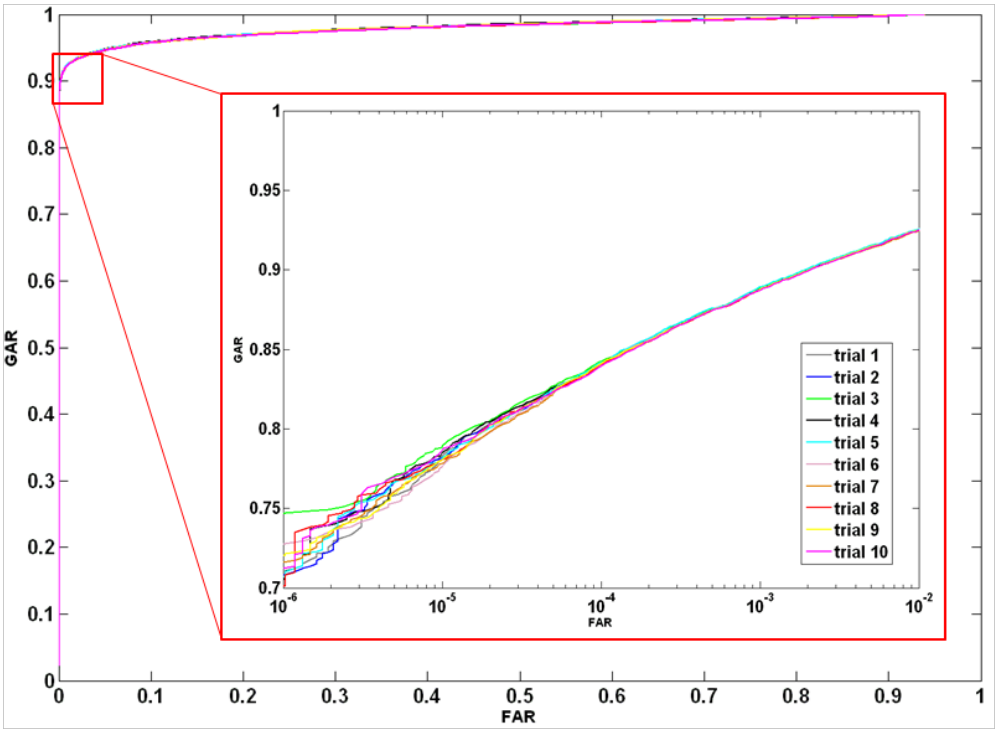


(c) Comparison of EER

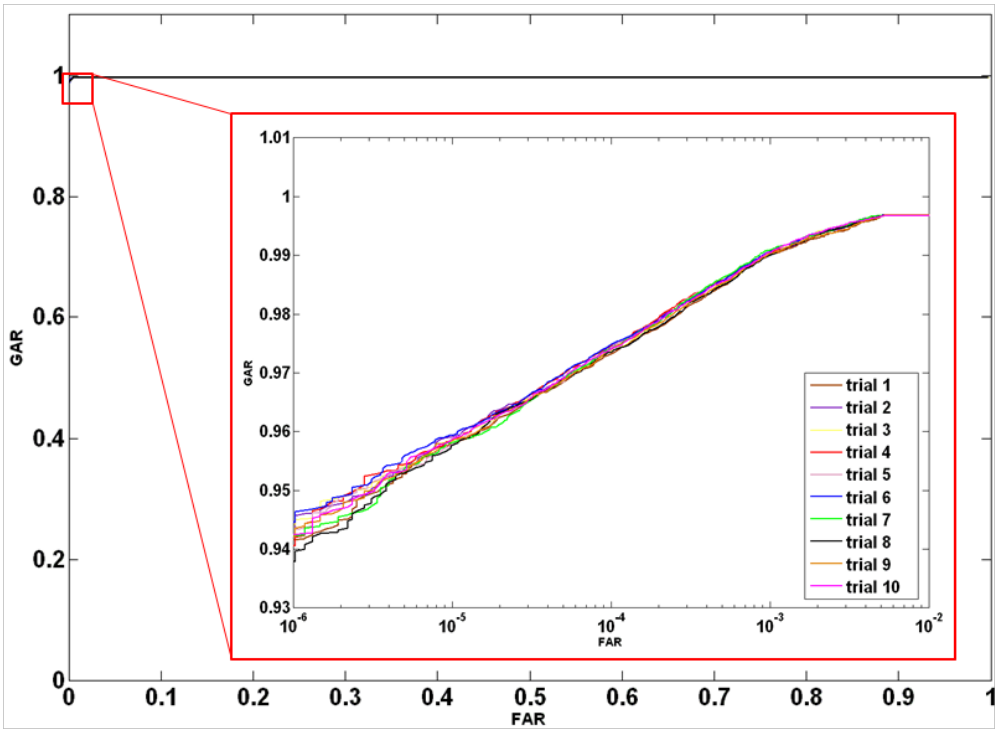
Fig. 5.6.: Continued

Table 5.3: Comparison of different matching algorithms for IUPUI Database

Algorithm	Image #	EER	GAR at FAR = 0.1%	GAR at FAR = 0.01%
2-D Gabor	610(frontal-look)	1.79%	92.57%	88.56%
1-D Log-Gabor	610(frontal-look)	2.95%	92.35%	89.80%
Gabor Descriptor	610(frontal-look)	2.73%	92.63%	87.61%
The proposed cancelable approach(average result from 10 trials)	610(frontal-look)	0.23%	99.77%	98.81%

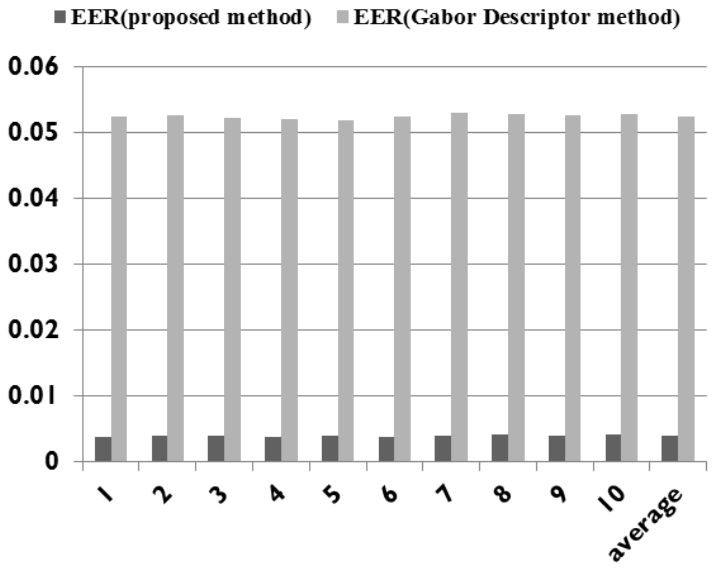


(a) ROC Curves of 10 Trials using Traditional Method (IUPUI)



(b) ROC Curves of 10 Trials using Proposed Method (IUPUI)

Fig. 5.7.: Result of experiment on entire IUPUI database



(c) Comparison of EER

Fig. 5.7.: Continued

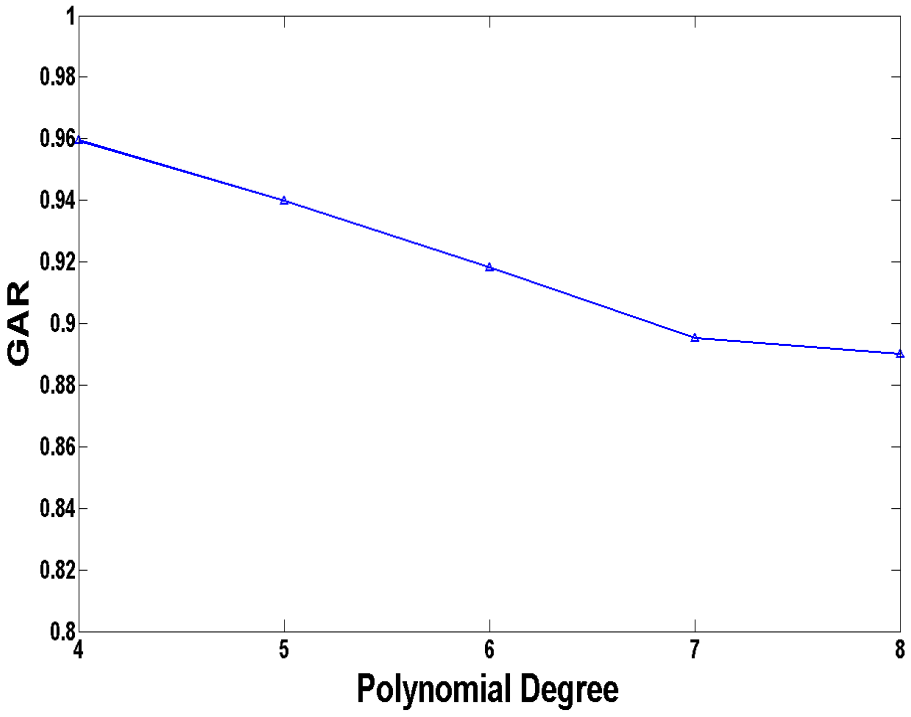


Fig. 5.8.: GAR at different polynomial degrees (FAR = 0)

6. CONCLUSIONS AND FUTURE WORK

There are mainly three contributions in this thesis: (1) a speed-up multi-stage non-cooperative iris recognition approach is proposed, (2) a key-incorporation-based non-cooperative iris recognition approach is proposed, and (3) a key-binding-based iris authentication approach is proposed.

The proposed speed-up multi-stage non-cooperative iris recognition approach makes use of the integral image and box filter to accelerate feature point detection similar to SURF method. Gabor wavelet based multi-scale local descriptor is applied to describe each detected feature point, which outperforms the other two popularly used local descriptors (SURF and DAISY) proved by the experimental results. A multi-stage matching algorithm is then applied to the generated multi-scale local descriptor. The high repeatability of detected feature point at large scales can be used to quickly separate different iris classes while the Gabor wavelet based descriptor can further detect details in iris texture pattern. The new designed multi-scale descriptor is shown to achieve high recognition accuracy even with low resolution off-angle iris images.

Based on the previous non-cooperative iris recognition approach, two security enhanced cancelable iris recognition are proposed to protect the iris template. The proposed key incorporated cancelable method achieves cancelability by applying a non-invertible transformation to the original sub-region based template. The user key information is incorporated with the transformed template by recording radial location of each feature point. The key-incorporated cancelable approach can achieve cancelability and also improve recognition accuracy, which is demonstrated by the experimental results on two databases (IUPUI and ICE).

The proposed key-binding scheme solves several limitations of the traditional fuzzy vault: the proposed method achieves cancelability by including a user specified external randomness to generate a cancelable template; the high stability of the large scale point location from two irises from the same class is utilized as the mutual information required by fuzzy vault scheme therefore error-correction code is no longer required to achieve stableness. The experimental results on ICE database shows that the proposed key-bind scheme can achieve 0 FAR and a very low FRR, which is very promising for high-security level applications using iris in the future.

There are some more work can be done in the future to improve the current approach. For the speed-up multi-stage non-cooperative iris recognition approach, a proper approximation of the Gabor filter used in feature description using a set of box filters can be applied to further increase the descriptor generation speed without reducing the accuracy too much. More experiments can be done on other databases to show the effectiveness of this approach. For the key-binding system, more mutual information between two irises can be extracted to increase the degree of the polynomial so that the scheme can provide more flexibility in more secure applications with longer key.

LIST OF REFERENCES

LIST OF REFERENCES

[1] J. Woodward, N. M. Orlans, and P. T. Higgins, *Biometrics*. McGraw-Hill, 2002.

[2] J. Daugman, "New methods in iris recognition," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 37, no. 5, pp. 1167–1175, 2007.

[3] J. Choi, W. De Neve, K. Plataniotis, and Y. Ro, "Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks," *Multimedia, IEEE Transactions on*, no. 99, pp. 1–1.

[4] Z. Lei, S. Liao, M. Pietikainen, and S. Li, "Face recognition by exploring information jointly in space, scale and orientation," *Image Processing, IEEE Transactions on*, vol. 20, no. 1, pp. 247–256, 2011.

[5] J. Feng and A. Jain, "Fingerprint reconstruction: from minutiae to phase," *IEEE transactions on pattern analysis and machine intelligence*, pp. 209–223, 2010.

[6] Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," *IEEE transactions on pattern analysis and machine intelligence*, pp. 72–87, 2010.

[7] A. Kumar and D. Zhang, "Improving biometric authentication performance from the user quality," *Instrumentation and Measurement, IEEE Transactions on*, vol. 59, no. 3, pp. 730–735, 2010.

[8] A. Kumar and D. Zhang, "Hand-geometry recognition using entropy-based discretization," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 2, pp. 181–187, 2007.

[9] D. Zhang, G. Lu, W. Li, L. Zhang, and N. Luo, "Palmprint recognition using 3-d information," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 39, no. 5, pp. 505–519, 2009.

[10] A. Jain and J. Feng, "Latent palmprint matching," *IEEE transactions on pattern analysis and machine intelligence*, pp. 1032–1047, 2008.

[11] B. Erkmen, N. Kahraman, R. Vural, and T. Yildirim, "Conic section function neural network circuitry for offline signature recognition," *Neural Networks, IEEE Transactions on*, vol. 21, no. 4, pp. 667–672, 2010.

[12] D. Hosseinzadeh and S. Krishnan, "Gaussian mixture modeling of keystroke patterns for biometric applications," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 38, no. 6, pp. 816–826, 2008.

[13] K. Moustakas, D. Tzovaras, and G. Stavropoulos, "Gait recognition using geometric features and soft biometrics," *Signal Processing Letters, IEEE*, vol. 17, no. 4, pp. 367–370, 2010.

[14] M. Goffredo, I. Bouchrika, J. Carter, and M. Nixon, "Self-calibrating view-invariant gait biometrics," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 40, no. 4, pp. 997–1008, 2010.

[15] J. Morales-Cordovilla, A. Peinado, V. Sánchez, and J. González, "Feature extraction based on pitch-synchronous averaging for robust speech recognition," *Audio, Speech, and Language Processing, IEEE Transactions on*, vol. 19, no. 3, pp. 640–651, 2011.

[16] A. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *Information Forensics and Security, IEEE Transactions on*, vol. 1, no. 2, pp. 125–143, 2006.

[17] J. Daugman, "Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons," *Proceedings of the IEEE*, vol. 94, no. 11, pp. 1927–1935, 2006.

[18] H. Proenca and L. Alexandre, "Toward noncooperative iris recognition: A classification approach using multiple signatures," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 607–612, 2007.

[19] N. Ratha, J. Connell, and R. Bolle, "An analysis of minutiae matching strength," in *Audio-and Video-Based Biometric Person Authentication*, pp. 223–228, Springer, 2001.

[20] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1–17, 2008.

[21] S. Parthasaradhi, R. Derakhshani, L. Hornak, and S. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 35, no. 3, pp. 335–343, 2005.

[22] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," *Information Forensics and Security, IEEE Transactions on*, vol. 1, no. 3, pp. 360–373, 2006.

[23] K. Nixon and R. Rowe, "Multispectral fingerprint imaging for spoof detection," in *Proceedings of SPIE*, vol. 5779, p. 214, 2005.

[24] K. Seifried, "How to hack: an introduction," vol. 9, pp. 44–47, 2000.

[25] A. Jain, P. Flynn, and A. Ross, *Handbook of biometrics*. Springer-Verlag New York Inc, 2008.

[26] K. Lam and D. Gollmann, "Freshness assurance of authentication protocols," *Computer SecurityESORICS 92*, pp. 259–271, 1992.

[27] K. Lam and T. Beth, "Timely authentication in distributed systems," *Computer SecurityESORICS 92*, pp. 293–303, 1992.

[28] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 15, no. 11, pp. 1148–1161, 1993.

[29] J. Daugman, "How iris recognition works," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 14, no. 1, pp. 21–30, 2004.

[30] R. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348–1363, 1997.

[31] J. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D. LoIacono, S. Mangru, M. Tinker, T. Zappia, and W. Zhao, "Iris on the move: Acquisition of images for iris recognition in less constrained environments," *Proceedings of the IEEE*, vol. 94, no. 11, pp. 1936–1947, 2006.

[32] C. Fancourt, L. Bogoni, K. Hanna, Y. Guo, R. Wildes, N. Takahashi, and U. Jain, "Iris recognition at a distance," in *Audio-and Video-Based Biometric Person Authentication*, pp. 1–13, Springer, 2005.

[33] R. Narayanswamy, G. Johnson, P. Silveira, and H. Wach, "Extending the imaging volume for biometric iris recognition," *Applied optics*, vol. 44, no. 5, pp. 701–712, 2005.

[34] Y. Du, E. Arslanturk, Z. Zhou, and C. Belcher, "Video-based noncooperative iris image segmentation," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, no. 99, pp. 1–11.

[35] E. Arvacheh and H. Tizhoosh, "Iris segmentation: Detecting pupil, limbus and eyelids," in *Image Processing, 2006 IEEE International Conference on*, pp. 2453–2456, IEEE, 2006.

[36] L. Ma, Y. Wang, and T. Tan, "Iris recognition using circular symmetric filters," in *Pattern Recognition, 2002. Proceedings. 16th International Conference on*, vol. 2, pp. 414–417, IEEE, 2002.

[37] J. Huang, L. Ma, Y. Wang, and T. Tan, "Iris recognition based on local orientation description," in *Proc. 6th Asian Conf. Computer Vision*, vol. 2, pp. 954–959, 2004.

[38] Y. Du, R. Ives, D. Etter, and T. Welch, "Use of one-dimensional iris signatures to rank iris pattern similarities," *Optical Engineering*, vol. 45, p. 037201, 2006.

[39] N. Schmid and J. Zuo, "On a methodology for robust segmentation of nonideal iris images.," *IEEE transactions on systems, man, and cybernetics. Part B, Cybernetics: a publication of the IEEE Systems, Man, and Cybernetics Society*, vol. 40, no. 3, p. 703, 2010.

[40] S. Shah and A. Ross, "Iris segmentation using geodesic active contours," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 4, pp. 824–836, 2009.

[41] L. Masek *et al.*, "Recognition of human iris patterns for biometric identification," *BE dissertation, School Comput. Sci. Software Eng., Univ. Western Australia, Perth, Australia*, 2003.

[42] K. Hollingsworth, K. Bowyer, and P. Flynn, "Pupil dilation degrades iris biometric performance," *Computer Vision and Image Understanding*, vol. 113, no. 1, pp. 150–157, 2009.

[43] V. Velisavljevic, "Low-complexity iris coding and recognition based on directionlets," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 3, pp. 410–417, 2009.

[44] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, and H. Nakajima, "An effective approach for iris recognition using phase-based image matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1741–1756, 2008.

[45] E. Krichen, S. Garcia-Salicetti, and B. Dorizzi, "A new phase-correlation-based iris matching for degraded images," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 39, no. 4, pp. 924–934, 2009.

[46] J. Thornton, M. Savvides, and B. Kumar, "A bayesian approach to deformed pattern matching of iris images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 596–606, 2007.

[47] D. Monro, S. Rakshit, and D. Zhang, "Dct-based iris recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 586–595, 2007.

[48] N. Sudha, N. Puhan, H. Xia, and X. Jiang, "Iris recognition on edge maps," *Computer Vision, IET*, vol. 3, no. 1, pp. 1–7, 2009.

[49] Z. Sun, Y. Wang, T. Tan, and J. Cui, "Improving iris recognition accuracy via cascaded classifiers," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 35, no. 3, pp. 435–441, 2005.

[50] R. Zhu, J. Yang, and R. Wu, "Iris recognition based on local feature point matching," in *Communications and Information Technologies, 2006. ISCIT'06. International Symposium on*, pp. 451–454, IEEE, 2006.

[51] L. Ma, T. Tan, Y. Wang, and D. Zhang, "Personal identification based on iris texture analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1519–1533, 2003.

[52] H. Proença and L. Alexandre, "Ubiris: A noisy iris image database," *Image Analysis and Processing–ICIAP 2005*, pp. 970–977, 2005.

[53] H. Proença, S. Filipe, R. Santos, J. Oliveira, and L. Alexandre, "The ubiris. v2: A database of visible wavelength iris images captured on-the-move and at-a-distance," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 32, no. 8, pp. 1529–1535, 2010.

[54] M. Vatsa, R. Singh, and A. Noore, "Improving iris recognition performance using segmentation, quality enhancement, match score fusion, and indexing," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 38, no. 4, pp. 1021–1035, 2008.

[55] Z. He, T. Tan, Z. Sun, and X. Qiu, "Toward accurate and fast iris segmentation for iris biometrics," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 31, no. 9, pp. 1670–1684, 2009.

[56] S. Schuckers, N. Schmid, A. Abhyankar, V. Dorairaj, C. Boyce, and L. Hornak, "On techniques for angle compensation in nonideal iris recognition," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 37, no. 5, pp. 1176–1190, 2007.

[57] C. Belcher and Y. Du, "Region-based sift approach to iris recognition," *Optics and Lasers in Engineering*, vol. 47, no. 1, pp. 139–147, 2009.

[58] Y. Du, C. Belcher, and Z. Zhou, "Scale invariant gabor descriptor-based noncooperative iris recognition," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, p. 37, 2010.

[59] D. Lowe, "Distinctive image features from scale-invariant keypoints," *International journal of computer vision*, vol. 60, no. 2, pp. 91–110, 2004.

[60] C. Harris and M. Stephens, "A combined corner and edge detector," in *Alvey vision conference*, vol. 15, p. 50, Manchester, UK, 1988.

[61] P. Hsiao, C. Lu, and L. Fu, "Multilayered image processing for multiscale harris corner detection in digital realization," *Industrial Electronics, IEEE Transactions on*, vol. 57, no. 5, pp. 1799–1805, 2010.

[62] K. Mikolajczyk and C. Schmid, "A performance evaluation of local descriptors," *IEEE transactions on pattern analysis and machine intelligence*, pp. 1615–1630, 2005.

[63] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," *Computer Vision–ECCV 2006*, pp. 404–417, 2006.

[64] E. Tola, V. Lepetit, and P. Fua, "Daisy: An efficient dense descriptor applied to wide-baseline stereo," *IEEE transactions on pattern analysis and machine intelligence*, pp. 815–830, 2009.

[65] M. Brown and D. Lowe, "Invariant features from interest point groups," in *British Machine Vision Conference, Cardiff, Wales*, pp. 656–665, Citeseer, 2002.

[66] P. Phillips, K. Bowyer, P. Flynn, X. Liu, and W. Scruggs, "The iris challenge evaluation 2005," in *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on*, pp. 1–8, IEEE, 2008.

[67] J. Woodward, "Biometrics: Privacy's foe or privacy's friend?," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1480–1492, 1997.

[68] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *2009 30th IEEE Symposium on Security and Privacy*, pp. 188–203, IEEE, 2009.

[69] G. Piosenka and R. Chandos, "Unforgeable personal identification system," Feb. 12 1991. US Patent 4,993,068.

[70] S. Tulyakov, F. Farooq, S. Chikkerur, and V. Govindaraju, "Secure fingerprint matching by hashing localized information," Mar. 2 2007. US Patent App. 11/713,123.

[71] Y. Rachlin, "Biometric processing using random projection transformations," 2010. US Patent App.0066493.

[72] A. Lumini and L. Nanni, "An improved biohashing for human authentication," *Pattern Recognition*, vol. 40, no. 3, pp. 1057–1065, 2007.

[73] A. Jin, D. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[74] A. Teoh and D. Ngo, "Cancellable biometerics featuring with tokenised random number," *Pattern recognition letters*, vol. 26, no. 10, pp. 1454–1460, 2005.

[75] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM conference on Computer and communications security*, pp. 28–36, ACM, 1999.

[76] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[77] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, pp. 1081–1088, 2006.

[78] A. Nagar, K. Nandakumar, and A. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, pp. 1–4, IEEE, 2008.

[79] K. Nandakumar, A. Nagar, and A. Jain, "Hardening fingerprint fuzzy vault using password," *Advances in Biometrics*, pp. 927–937, 2007.

[80] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in cryptology-Eurocrypt 2004*, pp. 523–540, Springer, 2004.

[81] Y. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," in *Multimedia and Expo, 2004. ICME'04. 2004 IEEE International Conference on*, vol. 3, pp. 2203–2206, IEEE, 2004.

[82] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 503–512, 2007.

[83] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Fuzzy extractors for continuous distributions," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 353–355, ACM, 2007.

[84] Q. Li and E. Chang, "Robust, short and sensitive authentication tags using secure sketch," in *Proceedings of the 8th workshop on Multimedia and security*, pp. 56–61, ACM, 2006.

[85] J. R. N. Connell and Z. J., "Salting system and method for cancelable iris biometrics," 2010. US Patent App.0046808.

[86] M. Savvides, B. Kumar, and P. Khosla, "Cancelable biometric filters for face recognition," *Pattern Recognition*, vol. 3, pp. 922–925, 2004.

[87] V. Govindaraju, V. Chavan, and S. Chikkerur, "Biometric convolution using multiple biometrics," Aug. 19 2005. US Patent App. 20,060/078,171.

[88] P. Griffin, "System,method and program production for recording creation of a cancelable biometric reference template in a biometric event journal record," 2010. US Patent App. 2010/0205660.

[89] R. Bolle, J. Connell, N. Ratha, and L. Percello, "Business system and method using a distorted biometrics," July 21 2003. US Patent App. 10/623,926.

[90] J. R. N. Connell and Z. J., "Registration-free transformation for cancelable iris biometrics," 2010. US Patent App. 2010/0046805.

[91] R. Bolle, N. Ratha, and J. Connell, "Method, apparatus and computer program product implementing anonymous biometric matching," Nov. 13 2007. US Patent App. 20,090/123,034.

[92] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 561–572, 2007.

[93] K. Yang and Y. Du, "Review of recent patents on cancelable biometrics," *Recent Patents on Electrical Engineering*, pp. 125–132, 2011.

[94] K. Yang, Y. Sui, Z. Zhou, Y. Du, and X. Zou, "A new approach for cancelable iris recognition," in *Proceedings of SPIE*, vol. 7708, p. 77080A, 2010.

[95] K. Yang, Y. Du, Z. Zhou, and C. Belcher, "Gabor descriptor based cancelable iris recognition method," in *Image Processing (ICIP), 2010 17th IEEE International Conference on*, pp. 4085–4088, IEEE, 2010.

[96] A. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of applied cryptography*. CRC, 1997.

[97] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for fingerprints," in *Audio-and Video-Based Biometric Person Authentication*, pp. 310–319, Springer, 2005.

[98] Y. Lee, K. Bae, S. Lee, K. Park, and J. Kim, "Biometric key binding: Fuzzy vault based on iris images," *Advances in Biometrics*, pp. 800–808, 2007.

[99] S. Yang and I. Verbauwhede, "Secure fuzzy vault based fingerprint verification system," in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, vol. 1, pp. 577–581, IEEE, 2004.